Mise À Niveau Sécurisée Des Points D'Accès, Évitant La Corruption D'Image Qui Provoque Une Boucle De Démarrage

Table des matières

Introduction

Certains points d'accès Cisco peuvent télécharger une image corrompue via CAPWAP à partir d'un contrôleur de la gamme 9800. Selon la version du logiciel de l'AP, l'AP peut essayer de démarrer l'image corrompue, résultant en une boucle de démarrage. Cet article explique quels modèles de points d'accès et quels chemins réseau sont susceptibles d'être corrompus par une image et comment effectuer une mise à niveau en toute sécurité.

Si vos AP sont maintenant dans une boucle de démarrage en raison de ce problème, consultez l'article Récupérer d'une boucle de démarrage causée par la corruption d'image sur les points d'accès Wave 2 et 11ax (CSCvx32806) pour des conseils sur les étapes de récupération.

Comment savoir si une mise à niveau est sensible à la corruption d'image

Vos points d'accès peuvent être susceptibles de télécharger un logiciel corrompu, puis d'essayer de démarrer ce logiciel, si les conditions suivantes se rapportent à votre déploiement :

Produits non affectés

- Contrôleurs LAN sans fil (WLC) : les points d'accès qui téléchargent depuis les contrôleurs LAN sans fil AireOS ne sont pas affectés
- Mobility Express, contrôleur sans fil intégré

- Points d'accès : les points d'accès Aironet 1800/1540/1100AC Wave 2 11ac et Wave1 11ac (1700/2700/3700/1570/IW3700) ne sont pas affectés (même si ces points d'accès s'enregistrent auprès de 9800 WLC, ils ne le sont pas)
- Points d'accès Wi-Fi 6E introduits depuis 2023 : IW9167, IW9165, C9163

Produits concernés

- WLC : le téléchargement des points d'accès à partir des contrôleurs LAN sans fil Cisco Catalyst 9800 peut être affecté
- Points d'accès : Les modèles de points d'accès suivants enregistrés sur les contrôleurs LAN sans fil de la gamme Cisco Catalyst 9800 sont affectés :
    - Points d'accès Aironet Wave2 11ac (2800/3800/4800/1560/IW6330/ESW6300)
    - Points d'accès Wi-Fi6 de la gamme Catalyst 9100 (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
    - Points d'accès Wi-Fi6E de la gamme Catalyst 9100 (9136/9162/9164/9166)

Versions touchées : le syndrome d'amorçage d'une mauvaise image

Ce problème, où l'AP tente de démarrer une image qu'il sait corrompue, est résolu par les ID de bogue Cisco suivants : CSCvx32806, CSCwc72021, CSCwd90081, qui sont corrigés dans les versions suivantes :

- 8.10.185.0 et versions ultérieures
- 17.3.7 et versions ultérieures
- 17.6.6 et versions ultérieures
- 17.9.3 et versions ultérieures
- 17.11.1 et versions ultérieures

Une fois que le point d'accès est mis à niveau vers le logiciel avec les correctifs ci-dessus, il peut toujours télécharger une image corrompue. Cependant, il ne tentera pas de démarrer cette image, mais il continuera plutôt de tenter le téléchargement jusqu'à ce qu'il réussisse.

Chemins réseau affectés

Le problème de corruption d'image AP n'a pas été vu avec un chemin LAN entre le 9800 et les AP - c'est-à-dire les chemins avec un MTU IP complet de 1500 octets, avec une faible latence et une perte de paquets très faible ne sont pas affectés. Le problème est plus susceptible de se produire sur des tunnels CAPWAP sur un WAN, avec les caractéristiques de chemin suivantes :

- perte de paquets élevée
- MTU CAPWAP faible (inférieur à 1 485 octets) : plus la MTU est faible, plus le risque est élevé
    - Une MTU CAPWAP faible peut être un symptôme de perte de paquets

Comment savoir si votre chemin réseau est en danger

- Sur le 9800, vérifiez CAPWAP Path MTU avec

```
<#root>

9800-L#show capwap detailed
Name          APMAC           SourceIP        SrcPort DestIP          DestPort

MTU

   Mode      McastIf
-------------------------------------------------------------------------------------------
Capwap1       D4AD.BDA2.8240 192.168.203.203 5247    192.168.6.100    5248

1485

  multicast Mc1
Capwap2       084F.F983.4A40 192.168.203.203 5247    192.168.6.103    5253

1005

  multicast Mc1
```

    - Si le MTU d'un AP donné fluctue, c'est un indicateur de risque fort
- Ou **show ap config general | inclure CAPWAP\ Chemin\ MTU** (dans show tech-support wireless)
    - Utilisez Wireless Config Analyzer Express (WCAE) sur la sortie « show tech-support wireless » du 9800 pour voir le MTU des points d'accès sous Access Points > Configuration
- Sur le modèle 9800, utilisez la commande « show ap uptime » et recherchez les points d'accès dotés d'une durée « AP Up Time » longue et d'une courte durée « Association Up Time »
    - S'il n'y a aucune raison pour que les AP aient un court temps d'association (c'est-à-dire pas de reconfiguration), cela peut indiquer un chemin réseau à risque

Comment mettre à niveau en toute sécurité à partir d'une version logicielle AP non fixée

---

Remarque : si votre déploiement est susceptible d'endommager l'image (c'est-à-dire les modèles de points d'accès affectés, l'exécution du logiciel sans le correctif pour le syndrome d'amorçage d'une image incorrecte, avec des caractéristiques WAN à risque), ne mettez pas à niveau en mettant simplement à niveau le logiciel 9800, et en faisant en sorte que les points d'accès rejoignent et téléchargent le nouveau logiciel - ils peuvent être sujets à l'endommagement de l'image et à l'entrée d'une boucle d'amorçage. Utilisez plutôt l'une des

---

méthodes suivantes :

Mise à niveau à l'aide d'un WLC local aux AP

Si possible, placez un contrôleur intermédiaire sur le LAN des AP - il peut s'agir d'un 9800-CL, ou (pour les AP Wave 2 / Wi-Fi 6) un AP en mode EWC, et mettez à niveau les AP vers la version cible. Ils pourront ensuite rejoindre le contrôleur de production en toute sécurité.

Mise à niveau via un contrôleur AireOS

Si vous avez un contrôleur AireOS exécutant 8.10.190.0 ou supérieur, et si vos modèles AP sont pris en charge par AireOS, joignez les AP à ce contrôleur. Cela permettra de mettre à niveau en toute sécurité les AP vers un logiciel fixe, et ils seront alors en mesure de joindre en toute sécurité le contrôleur de production.

Mise à niveau avec archive download-sw

Préparez la ou les images d'AP cible sur un serveur TFTP / SFTP qui est accessible aux AP de mise à niveau. Les mises à niveau d'image AP via TFTP ou SFTP ne sont pas soumises au problème de corruption d'image. Les AP peuvent initier une requête de téléchargement d'image à partir de l'interface de ligne de commande AP ou (si les AP sont joints au contrôleur) à partir de l'interface de ligne de commande du contrôleur.

1. Configurez un serveur TFTP ou SFTP dans un emplacement accessible aux points d'accès. Notez que les performances TFTP sont contrôlées par la latence, donc les téléchargements seront lents si le serveur TFTP est distant des AP. Comme le protocole SFTP utilise le protocole TCP, son débit sera bien meilleur si vous utilisez un chemin à latence élevée. Cependant, SFTP ne peut pas être déclenché à partir du WLC, car il nécessite une boîte de dialogue interactive pour entrer le nom d'utilisateur et le mot de passe.
2. Préparez les images AP souhaitées sur un serveur TFTP ou SFTP. Reportez-vous au Tableau 4 de la Matrice de compatibilité pour connaître la version 15.3(3)J* du point d'accès qui correspond à la version IOS-XE souhaitée, puis téléchargez la ou les images logicielles Lightweight AP appropriées pour le ou les modèles de point d'accès concernés depuis software.cisco.com.
    1. Par exemple, l'image AP 17.9.5 pour un CW9162 isap1g6b-k9w8-tar.153-3.JPN4.tar.
3. Pour effectuer une mise à niveau via l'interface de ligne de commande AP : si l'interface de ligne de commande AP est accessible via la console ou SSH :
    1. Entrez la commande TFTP ou SFTP :
       archive download-sw /no-reload tftp://<*adresse-ip*>/<*image*>
       ou
       archive download-sw /no-reload sftp://<*adresse-ip*>/<*image*>
       Nom d'utilisateur:*UTILISATEUR*
       Mot de passe : *XXX*
       L'image endommagée sera remplacée par l'image valide.
    2. Une fois le téléchargement de l'image terminé, émettez :
       redémarrage du capwap de test

Cela redémarrera le processus CAPWAP, afin que le point d'accès reconnaisse l'image nouvellement installée.

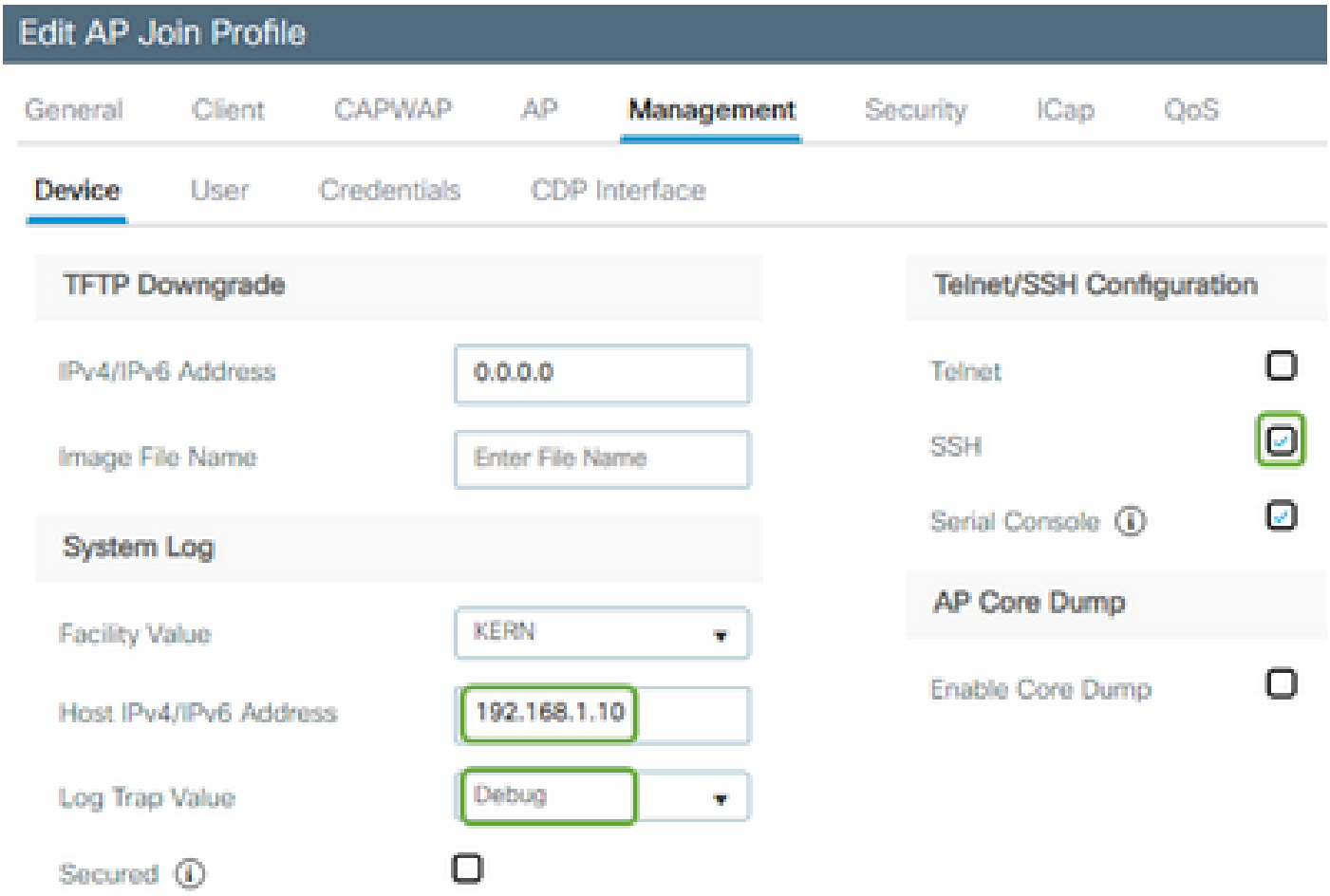
3. Pour mettre à niveau un grand nombre d'AP via "archive download-sw", plutôt que d'entrer la commande dans chaque AP individuellement, vous pouvez utiliser une méthode de script. Voir Mise à niveau AP via WLAN Poller ci-dessous.

4. Si les AP sont joints à un contrôleur, vous pouvez mettre à niveau les AP à partir de l'interface de ligne de commande du contrôleur (TFTP uniquement) :
    1. Dans IOS-XE :**ap nameAPNAMEtftp-*downgradeip.addr.of.server imagename.tar***
    2. Dans AireOS:**config ap tftp-*downgradeip.addr.of.server nomimage.tarAPNAME***
        1. Bien que les téléchargements CAPWAP depuis AireOS ne soient pas sujets à la corruption d'image, si vous prévoyez de migrer vos AP d'AireOS vers 9800, vous devriez d'abord télécharger une image AP avec les correctifs pour Alt-boot et le syndrome Boot a Bad Image (8.10.190.0 ou supérieur), avant de joindre les AP au 9800.
    3. Surveillez les journaux du serveur TFTP ou SFTP pour vérifier que chaque point d'accès a téléchargé correctement l'image. Une fois le téléchargement terminé, chaque point d'accès se recharge, exécutant l'image nouvellement téléchargée.

Mise à niveau des points d'accès via le prétéléchargement, surveillance des erreurs

Chargez l'image cible sur le 9800, et utilisez le prétéléchargement AP pour pousser la nouvelle image sur l'AP, tout en surveillant les instances de corruption d'image AP.

Étape 1. Vérifiez que SSH est activé sous le ou les profils de jonction AP sur le WLC C9800. Configurez un serveur Syslog sur le réseau. Configurez l'adresse IP du serveur syslog sous AP Join Profile pour tous les sites et définissez la valeur d'interruption du journal sur Debug. Vérifiez que le serveur syslog reçoit des syslogs du point d'accès.



Étape 2. Téléchargez l'image logicielle sur le WLC C9800 pour préparer le prétéléchargement via l'interface de ligne de commande :

```
C9800# copy tftp://x.x.x.x/C9800-80-universalk9_wlc.17.03.07.SPA.bin bootflash:
C9800# install add file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
```

Étape 3. Exécutez le prétéléchargement de l'image AP sur les WLC Cisco C9800 :

```
C9800# ap image predownload
```

Remarque : selon l'échelle et le type de déploiement, cette opération peut prendre de quelques minutes à quelques heures. Ne redémarrez pas le contrôleur ou les points d'accès tant que vous n'avez pas validé la validité de leurs images !

Étape 4. Une fois le pré-téléchargement pour tous les AP terminé, vérifiez l'un de ces deux messages de journal sur le serveur syslog :

- Vérification de la signature des images réussie.

- Échec de la vérification de la signature d'image : -3

Vérifiez également le résultat de la commande **`show ap image summary`**, en recherchant les instances de Failed to Download. Si le compteur est différent de zéro, alors trouvez les AP en échec via show ap image | inclure Échec.

Attention : si des points d'accès enregistrent l'échec de la vérification de la signature d'image, ou si des points d'accès n'ont pas pu être téléchargés, alors NE POURSUIVEZ PAS LE PROCESSUS DE MISE À NIVEAU. Si tous les AP affichaient le message «Image sign verify success», alors tous les AP ont correctement téléchargé l'image, et vous pouvez continuer en toute sécurité avec la mise à niveau 9800.

Étape 5. Si un AP a montré un échec de vérification ou n'a pas réussi à télécharger, alors, pour éviter une boucle de démarrage, vous devrez remplacer l'image dans la partition de sauvegarde de l'AP avec un téléchargement d'archive d'une image d'AP séparée en utilisant le processus suivant.

Si le nombre de points d'accès défaillants est faible, vous pouvez simplement envoyer une requête SSH à chaque point d'accès et lancer les étapes suivantes.

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
COS_AP#show version
COS_AP#test capwap restart
```

Remarque : « test capwap restart » est nécessaire pour que le processus CAPWAP de l'AP reconnaisse que l'image dans la partition de sauvegarde a été mise à jour. Cela provoquera une brève interruption du service, car la connexion CAPWAP avec le 9800 est redémarrée. S'il s'agit d'un problème opérationnel, cette étape peut être reportée à une fenêtre de maintenance.

Mise à niveau des AP avec WLAN Poller

Si le nombre de points d'accès à mettre à niveau via archive download-sw est important, vous pouvez utiliser un processus automatisé à l'aide du WLAN Poller.

Étape 1a. Installez le contrôleur WLAN sur un ordinateur Mac ou Windows.

Étape 1b. Remplissez le fichier csv de la liste d'applications avec les AP défaillants appropriés.

Étape 1c. Remplissez le fichier cmdlist avec les commandes ci-dessous (vous pouvez toujours en ajouter d'autres à votre discrétion) :

```
COS_AP#term mon
COS_AP#show clock
COS_AP#archive download-sw /no-reload tftp://<ip-address>/%apimage%
```

```
COS_AP#show version
COS_AP#test capwap restart
```

Étape 1d. Exécutez le contrôleur WLAN.

Étape 1e. Une fois son exécution terminée, veuillez vérifier le fichier journal de chaque AP pour valider la réussite de l'achèvement.

Étape 2. Activez immédiatement l'image sur le WLC C9800 et rechargez-la.

```
C9800#install activate file bootflash:C9800-80-universalk9_wlc.17.03.07.SPA.bin
- Confirm reload when prompted
```

Étape 3 : validation de l’image sur le WLC C9800 Si vous ignorez cette étape, le WLC reviendra à l'image logicielle précédente

```
C9800#install commit
```

Forum aux questions

Q. J'ai exécuté un prétéléchargement il y a quelques jours, mais je n'ai pas encore redémarré mon WLC et mes AP Cisco C9800. Je n'ai pas de syslog pour vérifier si l'image est corrompue. Comment puis-je vérifier si l'image est corrompue ?

A. Vérifiez show logging sur les AP/syslog. Si vous ne voyez aucun message de réussite ou d'échec dans la sortie de show logging, vous pouvez utiliser la commande "show flash syslogs" pour enregistrer la sortie syslog à partir de quand vous avez effectué le prétéléchargement. Si vous voyez le message "Signature d'image vérifier la réussite", alors vous savez que cet AP a téléchargé l'image avec succès.

Q : Je dispose d'un déploiement centralisé avec des points d'accès en mode local. Dois-je toujours exécuter les étapes répertoriées dans la section Solution/Solutions ?

R : Ce problème n'a été signalé que lors de la mise à niveau des AP sur une connexion WAN. Les points d'accès en mode local et sur des réseaux locaux sont très peu susceptibles de rencontrer ce problème, il n'est donc pas nécessaire de suivre cette procédure pour les mises à niveau, si vous êtes sûr qu'il y a très peu de perte de paquets entre le contrôleur et les points d'accès.

Q : J'ai de nouveaux AP prêts à l'emploi. Comment puis-je les déployer sans rencontrer ce problème ?

R : Les nouveaux points d'accès prêts à l'emploi téléchargeant du code sur le WAN seront

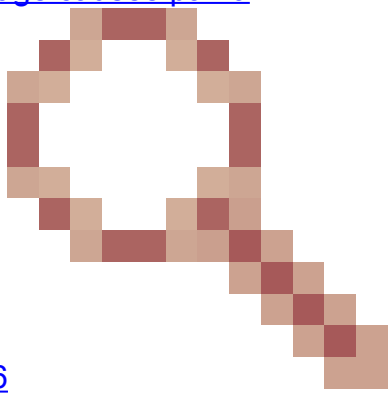
également sensibles à ce problème, sauf s'ils ont été fabriqués après décembre 2023.

Q : Que fait Cisco à long terme pour résoudre ce problème avec les téléchargements d'images CAPWAP du 9800 qui sont corrompus ?

R : Une fois que le point d'accès exécute déjà 17.11 ou plus, il peut utiliser la fonctionnalité de téléchargement d'image hors bande pour extraire l'image du contrôleur à l'aide de HTTPS. Le protocole TCP transmet les données de manière fiable, à l'aide d'une fenêtre glissante. Il est donc également beaucoup plus rapide sur un réseau étendu que le protocole CAPWAP (ou TFTP)

Q. J'ai des AP qui sont maintenant dans une boucle de démarrage. Comment puis-je les récupérer ?

R : Reportez-vous à l'article Récupérer à partir d'une boucle de démarrage causée par la corruption d'image sur les points d'accès Wave 2 et 11ax (CSCvx32806).



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.