Résolution des problèmes de sécurité liés à la plate-forme logicielle Cisco IOS-XE - août 2026

Table des matières

Introduction

Ce document décrit les bogues du logiciel sans fil signalés avec les versions de sécurité renforcée publiées pour l'avis Cisco IOS® XE d'août 2026.

Fond

Ce document fournit des conseils de mise à niveau pour répondre aux avis de sécurité, FN74383 et aux problèmes critiques.

Le 5 août 2026, Cisco a publié le document Cisco IOS XE Security Hardening Advisory qui a un impact sur plusieurs plates-formes, y compris, mais sans s'y limiter, les contrôleurs LAN sans fil de la gamme 9800. Comme l'indique la documentation, cet avis traite de plusieurs vulnérabilités découvertes en interne suite à une analyse complète de la sécurité interne par l'équipe d'ingénierie de Cisco IOS XE.

Plates-formes sans fil incluses dans la révision

Catalyst Wireless 9800 (C9800-L, C9800-CL, C9800-40, C9800-80)

WLC sans fil Cisco 9800 (CW9800L, CW9800M, CW9800H1/H2)

Sans fil 9800 intégré sur commutateur Catalyst (9800-SW) - prend uniquement en charge le déploiement SDA

Points d'accès de la gamme Catalyst 11ax 91xx basés sur COS (9105/9115/9117/9120/9130/9136/9164/9166)

Points d'accès sans fil Cisco 917x (CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Version du logiciel Cisco IOS XE	Première Version Fixe

17.9	17.9.10
17.12	17.12.8
17.15	17.15.6
17.18	17.18.4, 17.18.4a*
26.1	26.1.2

Tableau 1. Versions logicielles incluses dans la révision et versions durcies correspondantes

*Remarque : 17.18.4a prend en charge tous les WLC autonomes. Pour le contrôleur LAN sans fil intégré sur les commutateurs dans les déploiements SDA, utilisez le package sans fil 17.18.4 qui fonctionne avec la version de commutateur 17.18.4. Il n'existe pas de version 17.18.4a pour le commutateur ou le package sans fil.

Bogues critiques

Dans les versions renforcées pour la sécurité mentionnées dans le tableau 1, certains problèmes critiques ont été identifiés qui peuvent affecter votre utilisation de ces versions :

- ID de bogue Cisco CSCwv93265
- ID de bogue Cisco CSCwv98483

Détail des bogues critiques

ID de bogue Cisco CSCwv93265 :

Symptôme : Échecs de connectivité client ou d'itinérance lors de l'utilisation des fonctionnalités OpenRoaming, WPA3, 11k, 11v, 11r.

Plates-formes concernées : Tout le contrôleur sans fil Cisco 9800 et le package sans fil pour Cat9K.
Version du logiciel concerné : Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.18.4, Cisco IOS XE 17.15.6, Cisco IOS XE 17.12.8, Cisco IOS XE 17.9.10.
Un APSP correctif est disponible pour toutes les versions. Cisco recommande de déployer APSP sur tous les déploiements exécutant la version de sécurisation renforcée.

Remarque : Ce programme APSP est exceptionnellement disponible pour les clients

disposant de licences Essentials. Contactez le TAC pour qu'il soit publié au cas où vous ne pourriez pas le télécharger.

Version fixe :

	C9800-L	CW9800-L	C980-40	C980-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	Commutateurs cat9k	C9350	CEE-9100
17.15.6	APSP-Link	S. O.	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	S. O.	Cont le TA pour obter une conc spéc
17.18.4 bis	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	S. O.	S. O.	S. O.
17.18.4	S. O.	S. O.	S. O.	S. O.	S. O.	S. O.	S. O.	S. O.	APSP-Link	S. O.	S. O.
17.12.8	APSP-Link	S. O.	APSP-Link	APSP-Link	APSP-Link	S. O.	S. O.	S. O.	APSP-Link	S. O.	Pass train
26.1.2	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	liaison APSP	S. O.
17.9.10	APSP-Link	S. O.	APSP-Link	APSP-Link	APSP-Link	S. O.	S. O.	S. O.	APSP-Link	S. O.	Pass train

Tableau 2. Liaisons APSP pour différentes plates-formes WLC 9800

ID de bogue Cisco CSCwv98483

Symptôme : Les clients sans fil ancrés bloqués à IP_Learn lorsque C9800-L, CW9800-L, C9800-CL sont configurés comme WLC étranger.
Plates-formes concernées : C9800-L, CW9800-L, C9800-CL (uniquement dans le scénario Guest-Anchor où les plates-formes affectées agissent comme des WLC étrangers).
Version du logiciel concerné : Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6.
Solution de contournement: Activez le cryptage de liaison de données de mobilité au niveau du tunnel entre l'élément étranger et l'élément d'ancrage :

```
wireless mobility group member mac-address <peer_mac> ip <peer_ip> public-ip <peer_ip> group <peer_grou
```

Version fixe :

Product (produit)	C9800L	CW9800L	C9800-CL
17.15.6	SMU-Link	S. O.	SMU-LINK
17.18.4 bis	SMU-Link	SMU-Link	SMU-Link
26.1.2	SMU-Link	SMU-Link	SMU-Link

Conseils de mise à niveau pour les problèmes critiques et de conseil

Pour résoudre les problèmes critiques et de conseil signalés sur les versions sécurisées renforcées, Cisco recommande :

1. Les clients sans fil exécutant Cisco IOS XE version 17.12, 17.15, 17.18 passent aux étapes 2, 3 et 4. Les clients sans fil exécutant Cisco IOS XE version 17.9, 26.1, attendent que le correctif APSP soit publié sur cisco.com AVANT de procéder à la mise à niveau. Reportez-vous au Tableau 2 pour connaître les dates de publication des correctifs.
2. Avant la mise à niveau, exécutez les vérifications de mise à niveau et les étapes de récupération documentées ici pour atténuer l'impact dû à FN74383.
3. Mettez à niveau la version de sécurité renforcée de Cisco IOS XE et le correctif APSP dans la même fenêtre de maintenance pour éviter que le service sans fil ne soit affecté.
4. Si le bogue Cisco ayant l'ID CSCwv98483 a un impact, appliquez la solution de contournement jusqu'à ce que SMU devienne disponible. Une fois que SMU est publié, les clients doivent appliquer le correctif SMU.

Considérations relatives aux temps d'arrêt pour la planification Fenêtre de maintenance pour la mise à niveau + correctifs Cisco IOS XE

La mise à niveau de Cisco IOS XE sur les WLC 9800 configurés dans des configurations redondantes non redondantes ou haute disponibilité (HA) peut tirer parti de divers mécanismes tels que :

- Mise à niveau logicielle en service (ISSU)
- Mise à niveau continue N+1
- Mise à niveau unique

Pour plus de détails, référez-vous au Guide de démarrage rapide de mise à niveau WLC 9800.

En outre, les problèmes critiques nécessitent l'application de correctifs avec Software Maintenance Update (SMU) et Access Point Service Pack (APSP).

Pour plus de détails sur les différentes options de correctifs prises en charge par le WLC 9800, référez-vous au Guide de mise à niveau de correctifs et de points d'accès roulants pour le WLC 9800.

Pour planifier votre fenêtre de maintenance pour la mise à niveau + l'application de correctifs de Cisco IOS XE avec chaque mécanisme de mise à niveau, tenez compte des temps d'arrêt et de l'impact décrits dans cette section.

Mise à niveau logicielle en service (ISSU)

- Applicable uniquement à la paire de WLC 9800 fonctionnant en configuration HA SSO (HA Stateful Switchover) et uniquement prise en charge entre les catégories de versions à longue durée de vie et leurs versions de maintenance. (Non pris en charge sur les versions d'escalade et les trains de versions de courte durée sans versions de maintenance).
- ISSU offre une expérience de mise à niveau transparente en prenant en charge 9800 paires dans HA SSO tout en exécutant différentes versions logicielles et en exploitant la mise à niveau des points d'accès. Sur une paire HA 9800 opérationnelle, le WLC en veille est mis à niveau, et après SSO, le nouveau WLC en veille est mis à niveau. Pour plus de détails sur le processus ISSU et les interfaces de ligne de commande et les captures instantanées GUI correspondantes, référez-vous à Mise à niveau SSO 9800 HA utilisant ISSU.
- Exécutez les vérifications de mise à niveau et la récupération sur les points d'accès avant de lancer ISSU.
- Avec ISSU, la durée de la mise à niveau n'est pas facilement prévisible. En fonction de la taille du déploiement et de la vitesse du réseau, la mise à niveau peut prendre plusieurs heures.
- De plus, ISSU tire parti de la mise à niveau progressive des points d'accès où les points d'accès sont redémarrés de manière échelonnée pour minimiser les temps d'arrêt. Cependant, dans ce cas, cela signifie que les clients connectés aux AP exécutant la version renforcée continuent à rencontrer des problèmes de connectivité et d'itinérance documentés dans les ID de bogue Cisco CSCwv93265 et CSCwv98483 jusqu'à ce que le WLC soit corrigé après la mise à niveau ISSU.
- SMU pour l'ID de bogue Cisco CSCwv98483 est un correctif à froid qui nécessite un rechargement de WLC.
- APSP pour l'ID de bogue Cisco CSCwv93265 peut être appliqué à l'aide de la mise à niveau

de point d'accès roulant ou en une seule fois. Si vous utilisez la mise à niveau des points d'accès roulants, en fonction de la taille du déploiement, cela peut prendre plusieurs « heures » pour que tous les points d'accès soient mis à niveau et éviter définitivement les bogues critiques connus.
- Durée totale pendant laquelle le service peut être affecté (le WLC ou les points d'accès sont en panne OU la connectivité/l'itinérance du client est affectée) = Temps pour terminer l'ISSU + Temps pour le rechargement du WLC en raison du correctif à froid SMU + Temps pour la mise à niveau progressive des points d'accès pour APSP.

Mise à niveau des points d'accès permanents N+1

- Cette procédure s'appuie sur un WLC 9800 de rechange appelé N+1 WLC avec une version logicielle mise à niveau vers des AP hôtes tandis que la paire 9800 de « production » ou 9800 autonome subit une mise à niveau. Il est recommandé que ce WLC N+1 9800 n'ait aucun point d'accès enregistré AVANT le lancement de la mise à niveau progressive N+1.
- Exécutez les vérifications de mise à niveau et la récupération sur les AP pendant qu'ils sont enregistrés sur le WLC principal.
- Pour plus de détails sur le processus et les instantanés CLI et GUI associés, référez-vous à Mise à niveau du WLC 9800 en utilisant la mise à niveau du point d'accès roulant N+1.
- Dans ce processus, pour que les AP passent de manière transparente du WLC principal au WLC N+1, la version du logiciel exécutée sur le WLC N+1 et pré-téléchargée sur les AP doit correspondre exactement.
- Le prétéléchargement vers les points d'accès est facilité par le téléchargement, mais PAS par l'activation de la version renforcée de Cisco IOS XE sur le WLC principal. Sans activation d'image, les correctifs logiciels ne peuvent pas être appliqués ou prétéléchargés sur les points d'accès. Ce qui signifie que le WLC N+1 ne peut pas être corrigé aussi bien.
- Même dans ce processus, comme ISSU, les points d'accès transférés vers le WLC N+1 continuent d'être à risque pour la connectivité des clients et les problèmes d'itinérance documentés dans les ID de bogue Cisco CSCwv93265 et CSCwv98483 jusqu'à ce que le WLC N+1 soit corrigé, après la fin de la mise à niveau du point d'accès roulant.
- SMU pour l'ID de bogue Cisco CSCwv98483 est un correctif à froid qui nécessite un rechargement de WLC.
- APSP pour l'ID de bogue Cisco CSCwv93265 peut être appliqué à l'aide de la mise à niveau de point d'accès roulant ou en une seule fois. Si vous utilisez la mise à niveau des points d'accès roulants, en fonction de la taille du déploiement, cela peut prendre plusieurs « heures » pour que tous les points d'accès soient mis à niveau et éviter définitivement les bogues critiques connus.
- Durée totale pendant laquelle le service peut être affecté (WLC ou points d'accès en panne OU connectivité/itinérance du client affectée) = Temps nécessaire à tous les points d'accès pour basculer vers un WLC N+1 + Temps de rechargement du WLC en raison d'un correctif à froid SMU + Temps de mise à niveau progressive des points d'accès pour APSP.
- Pour votre fenêtre de maintenance, prenez également en compte le temps nécessaire pour que le WLC N+1 soit mis à niveau vers les versions renforcées de Cisco IOS XE et pour que les points d'accès prétéléchargent la version renforcée de Cisco IOS XE à partir du WLC principal, bien que cela n'ait aucun impact sur le service.

Mise à niveau régulière N+1 des points d'accès - RECOMMANDÉE

- Cette procédure repose sur un appel de WLC 9800 de rechange en tant que WLC N+1 avec une version logicielle mise à niveau vers des AP hôtes tandis que la paire 9800 de « production » ou 9800 autonome subit une mise à niveau.
- La recommandation est que ce WLC 9800 de rechange n'ait pas de points d'accès enregistrés AVANT que la mise à niveau N+1 ne soit lancée.
- Le WLC N+1 de rechange peut être mis à niveau vers Cisco IOS XE renforcé activé et validé et corrigé avec APSP et SMU, en une seule fois. Si aucun point d'accès n'est enregistré, cela n'a pas d'impact sur le service, mais vous devez tenir compte du temps nécessaire au rechargement de plusieurs WLC lors de la planification de votre fenêtre de maintenance.
- Sur la GUI principale du WLC où les AP sont enregistrés, naviguez à Configuration > Tags and Profiles : Amorçage AP > Base principale.
    - Définissez l'adresse IP du WLC N+1 et de l'interface de gestion sans fil (WMI) comme adresse principale.
    - Définissez le nom WLC principal actuel et l'adresse IP WMI sous Secondaire.
- Utilisez des filtres regex pour migrer en masse les AP du WLC principal vers le WLC N+1.
- Une fois enregistrés sur le WLC N+1, les AP exécutent déjà une version renforcée de sécurité ainsi que des correctifs pour corriger les bogues critiques.

Durée totale pendant laquelle le service peut être affecté (WLC ou points d'accès désactivés OU connectivité/itinérance du client affectée) = Temps nécessaire aux points d'accès pour migrer du WLC principal vers le WLC N+1, qui est dicté par la vitesse du réseau entre le point d'accès et les WLC.

Mise à niveau en une seule opération - RECOMMANDÉE, si aucun WLC N+1 n'est présent

- Dans cette procédure, le WLC principal est mis à niveau (avec activation et engagement) vers la version renforcée de sécurité de Cisco IOS XE en une seule étape.
- Dans le cadre de l'activation d'image, le WLC principal est rechargé et tous les AP se réenregistrent auprès du WLC principal de mise à niveau et reçoivent la version renforcée de sécurité de Cisco IOS XE.
- Jusqu'à ce qu'APSP soit appliqué, les AP sont exposés à des problèmes de connectivité et d'itinérance client documentés dans les ID de bogue Cisco CSCwv93265 et CSCwv98483.

Durée totale pendant laquelle le service peut être affecté (WLC ou points d'accès sont en panne OU la connectivité/l'itinérance du client est affectée) = Temps nécessaire au rechargement du WLC principal + Temps nécessaire au téléchargement de la version renforcée de Cisco IOS XE du WLC principal sur CAPWAP et au réenregistrement sur le WLC principal. (Doublez ce temps si le correctif SMU est appliqué) + Temps nécessaire à tous les points d'accès pour télécharger le correctif APSP du WLC principal et pour se réenregistrer sur le WLC principal.

Foire aux questions

Les points d'accès sont-ils affectés par cet avis de sécurité ?

Les points d'accès basés sur COS ont été inclus dans l'examen de la sécurité et les correctifs correspondants sont incorporés dans les versions renforcées de Cisco IOS XE.

Quel est le risque pour les WLC AireOS ?

Les WLC AireOS n'ont pas été inclus dans l'examen de sécurité car ils ont atteint leur date de fin d'assistance (LDoS).

Existe-t-il une version qui inclut tous les correctifs afin qu'une seule action de mise à niveau puisse être effectuée ?

Cisco envisage cette possibilité et peut publier des informations supplémentaires si elles deviennent disponibles. Une version spéciale de signalisation est disponible et inclut le PAA sur demande du TAC. Cette version spéciale d'escalade ne permet pas d'installer d'autres SMU ou APSP sur elle et elle contient uniquement le correctif d'APSP1.

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.