

# IOS-XE-beveiligingsadvies verhelpen - augustus 2026 en gerelateerde kritieke problemen

## Inhoud

---

## Inleiding

Dit document loopt door de kritieke draadloze softwarefouten die zijn gemeld met de verharde beveiligingsreleases die zijn gepubliceerd om IOS-XE-advies aan te pakken - augustus 2026. Het biedt upgraderichtlijnen voor [beveiligingsadvies](#), [FN74383](#) en de kritieke problemen.

## Achtergrond

Op 5 augustus 2026 heeft Cisco [IOS-XE Security Hardening Advisory](#) uitgebracht die gevolgen heeft voor meerdere platforms, waaronder maar niet beperkt tot 9800-serie draadloze LAN-controllers. Zoals gedocumenteerd, richt dit advies zich op meerdere intern ontdekte kwetsbaarheden die het gevolg zijn van een uitgebreide interne beveiligingsbeoordeling door Cisco IOS-XE Engineering.

Draadloze platforms opgenomen in de beoordeling

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

Cisco Wireless 9800 WLC (CW9800L, CW9800M, CW9800H1/H2)

Ingebouwde Wireless 9800 op Catalyst Switch (9800-SW) - ondersteunt alleen SDA-implementatie

COS-gebaseerde Catalyst 11ax 91xx-reeks toegangspunten  
(9105/9115/9117/9120/9130/9136/9164/9166)

Cisco Wireless 917x-reeks toegangspunten  
(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

|                               |                      |
|-------------------------------|----------------------|
| Cisco IOS XE Software Release | Eerste vaste release |
|-------------------------------|----------------------|



|         |                           |                      |                           |                           |                      |                     |                      |                     |                           |                     |
|---------|---------------------------|----------------------|---------------------------|---------------------------|----------------------|---------------------|----------------------|---------------------|---------------------------|---------------------|
| bis     | <a href="#">Link</a>      | <a href="#">Link</a> | <a href="#">Link</a>      | <a href="#">Link</a>      | <a href="#">Link</a> |                     | <a href="#">Link</a> |                     |                           |                     |
| 17.18.4 | NA                        | NA                   | NA                        | NA                        | NA                   | NA                  | NA                   | NA                  | <a href="#">APSP-Link</a> | NA                  |
| 17.12.8 | <a href="#">APSP-Link</a> | NA                   | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | Gepland voor 15 aug  | NA                  | NA                   | NA                  | <a href="#">APSP-Link</a> | NA                  |
| 26.1.2  | Gepland voor 15 aug       | Gepland voor 15 aug  | Gepland voor 15 aug       | Gepland voor 15 aug       | Gepland voor 15 aug  | Gepland voor 15 aug | Gepland voor 15 aug  | Gepland voor 15 aug | Gepland voor 15 aug       | Gepland voor 15 aug |
| 17.9.10 | <a href="#">APSP-Link</a> | NA                   | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | Gepland voor 15 aug  | NA                  | NA                   | NA                  | <a href="#">APSP-Link</a> | NA                  |

Tabel 2. APSP-koppelingen voor verschillende 9800 WLC-platforms

### [CSCwv98483](#)

Symptoom: verankerde draadloze clients die vastzitten op IP\_Learn wanneer C9800-L, CW9800-L, C9800-CL zijn geconfigureerd als buitenlandse WLC

Betrokken platforms: C9800-L, CW9800-L, C9800-CL (alleen in het gast-ankerscenario waarbij de getroffen platforms als buitenlandse WLC fungeren)

Betrokken softwareversie: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6

Workaround: Enable Mobility Data-link encryptie in de tunnel tussen het vreemde en het anker:

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

Vaste release: Cisco werkt actief aan een vaste patch/koude SMU en klanten worden op de hoogte gebracht zodra deze beschikbaar komt (Gepland voor release: 21 augustus). Dit zal een koude SMU zijn die een WLC-herbelasting vereist.

## Upgradebegeleiding voor adviserende en kritieke kwesties

Om zowel de adviserende als de kritieke problemen die zijn gemeld bij beveiligde releases aan te pakken, raadt Cisco aan

Stap 1. Draadloze klanten met IOS-XE versie 17.12, 17.15, 17.18 gaan verder met stap 2, 3 en 4. Draadloze klanten die IOS-XE versie 17.9, 26.1 gebruiken, wachten tot de APSP-patch op [cisco.com](#) is geplaatst VOORDAT ze een upgrade uitvoeren. Zie tabel 2 voor de releasedatums van de pleister

Stap 2. Voer voorafgaand aan de upgrade de [hier](#) gedocumenteerde upgradecontroles en herstelstappen uit om de gevolgen van [FN74383](#) te beperken

Stap 3. Upgrade de beveiligde IOS-XE-versie en de APSP-patch in hetzelfde onderhoudsvenster om te voorkomen dat de draadloze service wordt beïnvloed.

Stap 4. Als dit wordt beïnvloed door [CSCwv98483](#), past u de tijdelijke oplossing toe totdat SMU beschikbaar komt. Zodra SMU is geplaatst, wordt van klanten verwacht dat ze SMU-patch toepassen.

## Overwegingen voor downtime bij het plannen van het onderhoudsvenster voor de upgrade naar IOS-XE + patches

IOS-XE-upgrade op 9800 WLC's die zijn geconfigureerd in redundante configuraties met niet-redundante of hoge beschikbaarheid (HA) kunnen gebruikmaken van verschillende mechanismen, zoals

- In-Service Software Upgrade (ISSU)
- N+1 Rolling Upgrade
- One-shot upgrade

Raadpleeg voor meer informatie de [snelstartgids voor de 9800 WLC-upgrade](#)

Bovendien moeten de kritieke problemen worden gepatcht met Software Maintenance Update (SMU) en Access Point Service Pack (APSP)

Raadpleeg de [Patching and Rolling AP Upgrade Guide for 9800 WLC voor](#) meer informatie over de verschillende patchopties die door de 9800 WLC worden ondersteund

Om uw onderhoudsvenster voor IOS-XE-upgrade + patching te plannen met elke upgrademechanismen, houdt u rekening met de downtime en impact die in deze sectie worden gedocumenteerd.

### In-Service Software Upgrade (ISSU)

- Alleen van toepassing op een 9800 WLC-paar dat wordt uitgevoerd in HA Stateful Switchover (HA SSO)-configuratie en alleen wordt ondersteund tussen langeafstandstreinen en hun onderhoudsversies. (Niet ondersteund bij escalatie vrijgave en kortstondige vrijgave treinen zonder onderhoudsvrijgave)
- ISSU biedt een naadloze upgrade-ervaring door 9800 paar HASSO te ondersteunen terwijl u verschillende softwareversies uitvoert en gebruikmaakt van een rollende AP-upgrade. Op een operationeel 9800 HA-paar wordt de stand-by WLC geüpgraded en na SSO wordt de nieuwe stand-by WLC geüpgraded. Raadpleeg [Upgrade 9800 HA SSO met ISSU voor](#) meer informatie over het ISSU-proces en de bijbehorende CLI's en GUI-momentopnamen
- Voer de upgradecontroles en het herstel uit op toegangspunten voordat u de ISSU start.
- Bij ISSU is er, afhankelijk van de grootte van de implementaties en de netwerksnelheid,

geen gedefinieerde maximale tijd om het beveiligde IOS-XE-image op WLC en alle toegangspunten te activeren en kan het in "uren" lopen voor grote implementaties.

- Verder maakt ISSU gebruik van een rollende AP-upgrade waarbij AP's gespreid opnieuw worden opgestart om downtime te minimaliseren. In dit geval betekent dit echter dat clients die zijn verbonden met AP's met een geharde release, connectiviteits- en roamingproblemen blijven ondervinden die zijn gedocumenteerd in [CSCwv93265](#) en [CSCwv98483](#) totdat WLC is gepatcht na de ISSU-upgrade.
- SMU voor [CSCwv98483](#) is een koude patch die WLC herladen vereist.
- APSP voor [CSCwv93265](#) kan worden toegepast met behulp van Rolling AP-upgrade of in één shot. Als u een upgrade van het Rolling AP gebruikt, kan dit, afhankelijk van de grootte van de implementatie, enkele "uren" duren voordat alle AP's zijn geüpgraded en bekende kritieke bugs zeker worden vermeden
- **Totale duur waarop de service kan worden beïnvloed (WLC of toegangspunten zijn niet beschikbaar OF de connectiviteit/roaming van de client wordt beïnvloed) = Tijd om ISSU te voltooien + Tijd voor herladen van WLC vanwege SMU-koude patch + Tijd voor rollende upgrade van toegangspunt voor APSP**

## N+1 Rolling AP-upgrade

- Deze procedure is gebaseerd op een reserve 9800 WLC genaamd N+1 WLC met geüpgradede softwareversie om AP's te hosten, terwijl de "productie" 9800 paar of 9800 standalone upgrade ondergaat. De aanbeveling is dat er voor deze N+1 9800 WLC geen toegangspunten zijn geregistreerd VOORDAT de N+1 rolling upgrade wordt gestart.
- Voer de upgradecontroles en het herstel uit op toegangspunten terwijl deze zijn geregistreerd bij de primaire WLC
- Raadpleeg [Upgrade 9800 WLC met N+1 Rolling AP-upgrade voor](#) meer informatie over het proces en de bijbehorende CLI- en GUI-momentopnamen
- In dit proces moet de softwareversie die wordt uitgevoerd op N+1 WLC en vooraf is gedownload naar AP's exact overeenkomen, zodat AP's naadloos kunnen overschakelen van primaire WLC naar de N+1 WLC.
- Predownload naar AP's wordt gefaciliteerd door het downloaden, maar NIET door het activeren van IOS-XE-geharde release op primaire WLC. Zonder beeldactivering kunnen softwarepatches niet worden toegepast of vooraf worden gedownload naar toegangspunten. Wat op zijn beurt betekent dat N + 1 WLC niet ook kan worden gepatcht.
- Zelfs in dit proces, zoals ISSU, blijven toegangspunten die naar N+1 WLC zijn overgezet, een risico lopen op problemen met de connectiviteit van clients en roaming die zijn gedocumenteerd in [CSCwv93265](#) en [CSCwv98483](#) totdat N+1 WLC is gepatcht, nadat de upgrade van Rolling AP is voltooid.
- SMU voor [CSCwv98483](#) is een koude patch die WLC herladen vereist.
- APSP voor [CSCwv93265](#) kan worden toegepast met behulp van Rolling AP-upgrade of in één shot. Als u een upgrade van het Rolling AP gebruikt, kan dit, afhankelijk van de grootte van de implementatie, enkele "uren" duren voordat alle AP's zijn geüpgraded en bekende kritieke bugs zeker worden vermeden
- **Totale duur waarop de service kan worden beïnvloed (WLC of AP's zijn niet beschikbaar OF de connectiviteit/roaming van de client wordt beïnvloed) = Tijd die nodig is voor alle AP's om over te schakelen naar N+1 WLC + Tijd voor WLC-herbelasting vanwege SMU-koude patch + Tijd voor AP-rollende upgrade voor APSP**
- Houd voor uw onderhoudsvenster ook rekening met de tijd die nodig is voor een upgrade van N+1 WLC naar IOS-XE-geharde releases en voor AP's om IOS-XE-geharde release van primaire WLC te downloaden, hoewel dit

geen van beide servicegevolgen heeft

## N+1 regelmatige AP-upgrade - AANBEVOLEN

- Deze procedure is gebaseerd op een reserve 9800 WLC-aanroep als N+1 WLC met geüpgradede softwareversie om AP's te hosten, terwijl een "productie" 9800-paar of 9800 standalone wordt geüpgraded.
- De aanbeveling is dat deze reserve 9800 WLC geen toegangspunten heeft geregistreerd VOORDAT de N + 1-rollende upgrade wordt gestart.
- De reserve N+1 WLC kan in één shot worden geüpgraded naar geharde IOS-XE geactiveerd en gecommitteerd en gepatcht met APSP en SMU. Als er geen toegangspunten zijn geregistreerd, heeft dit geen gevolgen voor de service, maar moet u rekening houden met de tijd die nodig is voor het opnieuw laden van meerdere WLC's bij het plannen van uw onderhoudsvenster
- Navigeer op de primaire WLC-GUI waar AP's zijn geregistreerd naar Configuration > Tags and Profiles: AP Priming > Primary Base
  - Definieer N+1 WLC en Wireless Management Interface (WMI) IP-adres als primair
  - Huidige primaire WLC-naam en WMI-IP definiëren onder Secundair
- Gebruik regex-filters om AP's in bulk te migreren van primaire WLC naar N+1 WLC.
- Eenmaal geregistreerd bij N + 1 WLC, zullen AP's al een beveiligde release uitvoeren, samen met patches om kritieke bugs te verhelpen.

Totale duur waarop de service van invloed kan zijn (WLC of AP's zijn niet beschikbaar OF de connectiviteit/roaming van de client wordt beïnvloed) = De tijd die nodig is voor AP's om van primaire WLC naar N+1 WLC te migreren, wordt bepaald door de netwerksnelheid tussen AP en WLC's.

## One-Shot Upgrade - AANBEVOLEN, indien geen N+1 WLC aanwezig

- In deze procedure wordt de primaire WLC in één stap geüpgraded (samen met activering en inzet) naar een beveiligde IOS-XE-release.
- Als onderdeel van de activering van het image wordt de primaire WLC opnieuw geladen en worden alle toegangspunten opnieuw geregistreerd bij de primaire WLC-upgrade en ontvangen ze de beveiligde IOS-XE-release.
- Totdat APSP wordt toegepast, lopen AP's het risico op problemen met de clientconnectiviteit en roaming die zijn gedocumenteerd in [CSCwv93265](#) en [CSCwv98483](#)

Totale duur waarop de service van invloed kan zijn (WLC of AP's zijn niet beschikbaar OF de connectiviteit/roaming van de client wordt beïnvloed) = Tijd die nodig is voor primaire WLC om opnieuw te laden + Tijd die nodig is voor alle AP's om een geharde IOS-XE-release van primaire WLC via CAPWAP te downloaden en zich terug te registreren bij primaire WLC. (Verdubbel deze tijd als SMU-patch wordt toegepast) + Tijd die nodig is voor alle AP's om een APSP-patch van primaire WLC te downloaden en zich terug te registreren bij primaire WLC.

# Veelgestelde vragen

Q1. Worden de toegangspunten beïnvloed door dit beveiligingsadvies?

COS-gebaseerde toegangspunten werden opgenomen in de beveiligingsbeoordeling en de bijbehorende oplossingen zijn opgenomen in de geharde IOS-XE-releases

Q2. Wat is het risico voor AireOS WLC's?

AireOS WLC's zijn niet opgenomen in de beveiligingsbeoordeling, omdat het de laatste dag van ondersteuning (LDoS) heeft bereikt

## 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.