

IOS-XE Security Advisory vom August 2026 und damit verbundenen kritischen Problemen beheben

Inhalt

Einleitung

In diesem Dokument werden die kritischen Fehler in der Wireless-Software behandelt, die in den veröffentlichten Versionen für robuste Sicherheit für das IOS-XE-Gutachten vom August 2026 gemeldet wurden. Es bietet Upgrade-Anleitungen für die [Sicherheitsberatung, FN74383](#) und die kritischen Probleme.

Hintergrund

Am 5. August 2026 hat Cisco einen [IOS-XE Security Hardening Advisory](#) veröffentlicht, der sich auf mehrere Plattformen auswirkt, einschließlich, aber nicht beschränkt auf, Wireless LAN Controller der Serie 9800. Wie dokumentiert, behebt dieser Ratgeber mehrere intern entdeckte Schwachstellen, die sich aus einer umfassenden internen Sicherheitsüberprüfung durch Cisco IOS-XE Engineering ergeben haben.

Wireless-Plattformen im Test enthalten

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

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

Integriertes Wireless 9800 auf Catalyst Switch (9800-SW) - unterstützt nur SDA-Bereitstellung

COS-basierte Catalyst Access Points der Serie 11ax 91xx
(9105/9115/9117/9120/9130/9136/9164/9166)

Cisco Wireless Access Points der Serie 917x
(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Cisco IOS XE Softwareversion	Erste feste Version
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

Tabelle 1. In der Prüfung enthaltene Software-Versionen und entsprechende Versionen mit eingeschränkter Funktionalität



* Hinweis: 17.18.4a unterstützt alle Standalone-WLCs. Verwenden Sie nur für den integrierten Wireless LAN Controller auf Switches in SDA-Bereitstellungen das Wireless-Paket 17.18.4, das mit der Switch-Version 17.18.4 kompatibel ist. Es wird keine Version 17.18.4a für den Switch oder das Wireless-Paket geben.

Kritische Fehler

In den sicherheitsoptimierten Versionen, die in Tabelle 1 erwähnt sind, wurden einige kritische Probleme identifiziert, die sich auf Ihre Verwendung dieser Versionen auswirken können.

1. [CSCwv 93265](#)
2. [CSCwv 98483](#)

Kritische Fehler im Detail

[CSCwv 93265](#)

Symptom: Client-Verbindungen oder Roaming-Fehler beim Einsatz von OpenRoaming-, WPA3-, 11k-, 11v- und 11r-Funktionen

Betroffene Plattformen: Alle Cisco Wireless Controller und Wireless-Pakete der Serie 9800 für Cat9K.

Betroffene Softwareversion: 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

Nächster Schritt: Für 17.12.8, 17.15.6 und 17.18.4a steht ein korrigierender APSP zur Verfügung. Die Korrektur-APSP für andere IOS-XE-Versionen (17.9.10, 26.1.2) soll bis zum 15. August veröffentlicht werden. Cisco empfiehlt die Bereitstellung von APSP, sobald APSP freigegeben wird.

Feste Version:

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	Cat9k-Switches	C9350
17.15.6	APSP-	NA	APSP-	APSP-	APSP-	APSP-Link	APSP-	APSP-Link	APSP-Link	NA

	Link		Link	Link	Link		Link			
17,18,4a	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	NA
17.18.4	NA	NA	NA	NA	NA	NA	NA	NA	APSP-Link	NA
17.12.8	APSP-Link	NA	APSP-Link	APSP-Link	Geplant für den 15. August	NA	NA	NA	APSP-Link	NA
26.1.2	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August	Geplant für den 15. August
17.9.10	APSP-Link	NA	APSP-Link	APSP-Link	Geplant für den 15. August	NA	NA	NA	APSP-Link	NA

Tabelle 2. APSP-Links für verschiedene 9800 WLC-Plattformen

[CSCwv 98483](#)

Symptom: Verankerte Wireless-Clients bleiben bei IP_Learn hängen, wenn C9800-L, CW9800-L, C9800-CL als ausländischer WLC konfiguriert sind

Betroffene Plattformen: C9800-L, CW9800-L, C9800-CL (nur im Guest-Anchor-Szenario, bei dem die betroffenen Plattformen als fremder WLC fungieren)

Betroffene Softwareversion: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6

Problemumgehung: Aktivieren Sie die Mobility Data-Link-Verschlüsselung im Tunnel zwischen dem Fremd- und dem Ankerpunkt:

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

Feste Version: Cisco arbeitet aktiv an einer SMU für feste Patches/Kaltinstallationen, und die Kunden werden benachrichtigt, sobald diese verfügbar sind (geplant für die Veröffentlichung: 21. August). Hierbei handelt es sich um eine kalte SMU, die ein erneutes Laden des WLC erfordert.

Upgrade-Leitfaden für Hinweise und kritische Probleme

Cisco empfiehlt zur Bewältigung der beratenden und kritischen Probleme bei sicherheitsoptimierten Versionen,

Schritt 1: Wireless-Kunden mit IOS-XE Version 17.12, 17.15, 17.18 fahren mit den Schritten 2, 3 und 4 fort. Wireless-Kunden mit IOS-XE Version 17.9, 26.1 warten, bis der APSP-Patch auf [cisco.com](#) gepostet wird, BEVOR Sie ein Upgrade durchführen. Die Veröffentlichungsdaten für Patches finden Sie in Tabelle 2.

Schritt 2: Führen Sie vor dem Upgrade die [hier](#) beschriebenen Upgrade-Prüfungen und Wiederherstellungsschritte aus, um die Auswirkungen von [FN74383](#) zu mindern.

Schritt 3: Führen Sie im selben Wartungsfenster ein Upgrade der gesicherten IOS-XE-Version und des APSP-Patches durch, um zu verhindern, dass der Wireless-Service beeinträchtigt wird.

Schritt 4: Wenn [CSCwv98483](#) dies [beeinträchtigt](#), wenden Sie die Problemumgehung an, bis SMU verfügbar ist. Sobald SMU bereitgestellt ist, werden die Kunden voraussichtlich einen SMU-Patch anwenden.

Überlegungen zu Ausfallzeiten bei der Planung des Wartungsfensters für IOS-XE-Upgrade + Patches

IOS-XE-Upgrade auf 9800 WLCs, die in nicht redundanten oder hochverfügbaren redundanten Konfigurationen konfiguriert sind, kann verschiedene Mechanismen nutzen, z. B.

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

Weitere Informationen finden Sie in der [9800 WLC Upgrade Quick Start Guide](#)

Darüber hinaus erfordern die kritischen Probleme Patches mit dem Software Maintenance Update (SMU) und dem Access Point Service Pack (APSP).

Weitere Informationen zu den verschiedenen Patching-Optionen, die vom 9800 WLC unterstützt werden, finden Sie im [Patching and Rolling AP Upgrade Guide for 9800 WLC](#).

Um Ihr Wartungsfenster für IOS-XE-Upgrade + Patching mit jedem Upgrade-Mechanismus zu planen, berücksichtigen Sie die in diesem Abschnitt dokumentierten Ausfallzeiten und Auswirkungen.

In-Service-Software-Upgrades (ISSU)

- Gilt nur für 9800 WLC-Paare, die in HA Stateful Switchover (HA SSO)-Konfiguration betrieben werden und nur zwischen langlebigen Release-Zügen und deren Wartungsversionen unterstützt werden. (Keine Unterstützung bei Eskalations-Releases und kurzfristigen Releases ohne Wartungsversionen)
- ISSU ermöglicht nahtlose Upgrades durch Unterstützung von 9800 Paar in HA SSO bei

gleichzeitiger Ausführung verschiedener Softwareversionen und Nutzung von rollierenden AP-Upgrades. Auf einem betriebsbereiten HA-Paar der Serie 9800 wird der Standby-WLC aktualisiert, und nach der SSO wird der neue Standby-WLC aktualisiert. Weitere Informationen zum ISSU-Prozess und den entsprechenden CLIs und GUI-Snapshots finden Sie unter [Upgrade 9800 HA SSO mit ISSU](#).

- Führen Sie die Upgrade-Prüfungen und die Wiederherstellung auf den APs aus, bevor Sie ISSU initiieren.
- Bei ISSU gibt es je nach Größe der Bereitstellungen und der Netzwerkgeschwindigkeit keine festgelegte Höchstzeit für die Aktivierung des gesicherten IOS-XE-Images auf dem WLC und allen APs. Bei großen Bereitstellungen kann dieser Zeitraum in Stunden überschritten werden.
- Darüber hinaus nutzt ISSU ein schrittweises AP-Upgrade, bei dem APs nach und nach neu gestartet werden, um Ausfallzeiten zu minimieren. In diesem Fall bedeutet dies jedoch, dass für Clients, die mit APs verbunden sind, auf denen eine robuste Version ausgeführt wird, weiterhin Verbindungs- und Roaming-Probleme auftreten, die in [CSCwv93265](#) und [CSCwv98483](#) dokumentiert sind, bis WLC nach dem ISSU-Upgrade gepatcht wird.
- SMU für [CSCwv98483](#) ist ein kalter Patch, der WLC neu laden muss.
- APSP für [CSCwv93265](#) kann mithilfe eines Rolling AP-Upgrades oder in einer Momentaufnahme angewendet werden. Bei Verwendung eines Rolling AP-Upgrades kann es je nach Größe der Bereitstellung mehrere "Stunden" dauern, bis alle Access Points aktualisiert sind und bekannte kritische Fehler definitiv vermieden werden.
- **Gesamtdauer, während der der Service beeinträchtigt sein könnte (WLC oder APs sind ausgefallen ODER Client-Konnektivität/Roaming ist beeinträchtigt) = Zeit bis zum Abschluss des ISSU + Zeit für das erneute Laden des WLC aufgrund des SMU Cold Patches + Zeit für das AP-Roll-Upgrade für APSP**

N+1 Rolling AP-Upgrade

- Dieses Verfahren basiert auf einem Ersatz-9800-WLC, der als N+1-WLC mit aktualisierter Softwareversion für Host-APs bezeichnet wird, während ein Upgrade des Produktions-9800-Paars oder der eigenständigen 9800-Serie durchgeführt wird. Es wird empfohlen, für diesen N+1-9800-WLC keine APs zu registrieren, BEVOR das N+1-Rolling-Upgrade initiiert wird.
- Führen Sie die Upgrade-Prüfungen und die Wiederherstellung auf den APs aus, während diese beim primären WLC registriert sind.
- Weitere Informationen zum Prozess und den zugehörigen CLI- und GUI-Snapshots finden Sie unter [Upgrade 9800 WLC using N+1 Rolling AP upgrade \(Upgrade für N+1-Rolling-AP\)](#).
- Damit die APs nahtlos vom primären WLC auf den N+1 WLC umgestellt werden können, muss die Softwareversion, die auf dem N+1 WLC ausgeführt und auf die APs vorinstalliert wird, genau übereinstimmen.
- Das Vorabdownload auf APs wird durch Herunterladen erleichtert, jedoch NICHT durch Aktivieren der verstärkten IOS-XE-Version auf dem primären WLC. Ohne Image-Aktivierung können Software-Patches nicht auf APs angewendet oder vorab heruntergeladen werden. Das wiederum bedeutet, dass N+1 WLC nicht auch gepatcht werden kann.
- Auch in diesem Prozess sind, wie bei ISSU, APs, die auf N+1 WLC umgestellt werden, weiterhin in Bezug auf Client-Konnektivitäts- und Roaming-Probleme gefährdet, die in [CSCwv93265](#) und [CSCwv98483](#) dokumentiert sind, bis N+1 WLC gepatcht ist, nachdem das Rolling AP-

Upgrade abgeschlossen ist.

- SMU für [CSCwv98483](#) ist ein kalter Patch, der WLC neu laden muss.
- APSP für [CSCwv93265](#) kann mithilfe eines Rolling AP-Upgrades oder in einer Momentaufnahme angewendet werden. Bei Verwendung eines Rolling AP-Upgrades kann es je nach Größe der Bereitstellung mehrere "Stunden" dauern, bis alle Access Points aktualisiert sind und bekannte kritische Fehler definitiv vermieden werden.
- **Gesamtdauer, während der der Service beeinträchtigt sein könnte (WLC oder APs sind ausgefallen ODER Client-Konnektivität/Roaming ist beeinträchtigt) = Dauer des Rollovers aller APs auf N+1 WLC + Zeit für das Neuladen des WLC aufgrund des SMU Cold Patches + Zeit für das AP-Rollover-Upgrade für APSP**
- Berücksichtigen Sie für Ihr Wartungsfenster auch die Zeit, die für das Upgrade von N+1 WLC auf IOS-XE-Version (Härtung) und für das Vorabdownload der Härtung von IOS-XE vom primären WLC durch die APs benötigt wird, auch wenn keines der beiden Ereignisse Auswirkungen auf den Service hat.

N+1 Reguläres AP-Upgrade - EMPFOHLEN

- Bei diesem Verfahren wird ein 9800-WLC-Ersatzruf als N+1-WLC mit aktualisierter Softwareversion zum Hosten von APs verwendet, während die "Produktions"-Switches der Serie 9800 oder die Serie 9800 als Standalone-Lösung aktualisiert werden.
- Es wird empfohlen, für diesen 9800 WLC-Ersatzteil keine APs zu registrieren, BEVOR das N+1-Rolling-Upgrade initiiert wird.
- Der N+1 WLC kann auf gehärtete IOS-XE-aktivierte Software aktualisiert und mit APSP und SMU in einem einzigen Mausklick aktiviert und aktiviert sowie mit Patches versehen werden. Da keine APs registriert sind, wirkt sich dies nicht auf die Services aus. Sie sollten jedoch die Zeit berücksichtigen, die zum erneuten Laden mehrerer WLC erforderlich ist, wenn Sie Ihr Wartungsfenster planen.
- Navigieren Sie auf der primären WLC-GUI, auf der die Access Points registriert sind, zu COnfiguration > Tags and Profiles: AP-Primierung > Primärbasis
 - N+1 WLC- und WMI-IP-Adresse (Wireless Management Interface) als primäre Adresse definieren
 - Aktuelle primären WLC-Namen und WMI-IP unter "Sekundär" definieren
- Verwendung von Regex-Filtern für die Massenmigration von APs vom primären WLC auf N+1 WLC.
- Nach der Registrierung bei N+1 WLC werden die APs bereits eine Version mit erhöhter Sicherheit sowie Patches zur Behebung kritischer Fehler ausführen.

Gesamtdauer, während der der Service beeinträchtigt sein könnte (WLC oder APs sind ausgefallen ODER Client-Konnektivität/Roaming ist beeinträchtigt) = Zeit, die die APs für die Migration vom primären WLC zum N+1 WLC benötigen. Dies wird durch die Netzwerkgeschwindigkeit zwischen AP und WLCs bestimmt.

One Shot Upgrade - EMPFOHLEN, falls kein N+1 WLC vorhanden

- Bei diesem Verfahren wird das Upgrade des primären WLC (zusammen mit der Aktivierung und der Verpflichtung) auf die IOS-XE-Version mit Sicherheitsfunktionen in einem Schritt

durchgeführt.

- Im Rahmen der Image-Aktivierung wird der primäre WLC neu geladen, und alle APs registrieren sich mit dem Upgrade des primären WLC und erhalten die sicherheitsoptimierte IOS-XE-Version.
- Bis zur Anwendung von APSP sind die APs durch Client-Verbindungs- und Roaming-Probleme gefährdet, die in [CSCwv9325](#) und [CSCwv98483](#) dokumentiert sind.

Gesamtdauer, während der der Service beeinträchtigt sein könnte (WLC oder APs sind ausgefallen ODER Client-Konnektivität/Roaming ist beeinträchtigt) = Zeit für das erneute Laden des primären WLC + Zeit für das Herunterladen der gehärteten IOS-XE-Version vom primären WLC über CAPWAP und für die Registrierung beim primären WLC. (Diese Zeit verdoppeln, wenn ein SMU-Patch angewendet wird) + Zeit für alle APs zum Herunterladen von APSP Patch vom primären WLC zu installieren und sich wieder beim primären WLC anzumelden.

Häufig gestellte Fragen

Frage 1: Sind die APs von dieser Sicherheitsempfehlung betroffen?

COS-basierte Access Points wurden in die Sicherheitsüberprüfung einbezogen und die entsprechenden Fixes in die robusten IOS-XE-Versionen integriert

Q2. Welches Risiko besteht für AireOS WLCs?

AireOS WLCs wurden nicht in die Sicherheitsüberprüfung einbezogen, da sie den letzten Support-Tag (Last Day of Support, LDoS) erreicht haben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.