Remediate IOS-XE Security Advisory - Aug 2026 and Related Critical Issues

Contents

Introduction

This document describes the critical wireless software bugs reported with the hardened security releases published for the IOS-XE advisory - Aug 2026.

Background

This document provides upgrade guidance to address Security Advisory, FN74383 and the critical issues.

On Aug 5th, 2026 Cisco released IOS-XE Security Hardening Advisory that impacts multiple platforms, including but not limited to, 9800 series Wireless LAN Controllers. As documented, this advisory addresses multiple internally discovered vulnerabilities resulting from a comprehensive internal security review by Cisco IOS-XE Engineering.

Wireless Platforms included in the review

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

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

Embedded Wireless 9800 on Catalyst Switch (9800-SW) - only supports SDA deployment

COS based Catalyst 11ax 91xx Series Access Points (9105/9115/9117/9120/9130/9136/9164/9166)

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

Cisco IOS XE Software Release	First Fixed Release
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

Table 1. Software Releases included in review and corresponding hardened releases

***Note**: 17.18.4a supports all the standalone WLCs. Only for the embedded Wireless Lan Controller on switches in SDA deployments use the 17.18.4 wireless package that will work with 17.18.4 switch release. There will not be a 17.18.4a version for switch or wireless package.

Critical Bugs

In the security hardened releases mentioned in Table 1, some critical issues have been identified that may affect your use of these releases.

1. CSCwv93265
2. CSCwv98483

Critical Bugs in Detail

CSCwv93265
Symptom: Client Connectivity or Roaming Failures when OpenRoaming, WPA3, 11k, 11v, 11r features are in use.
Affected Platforms: All Cisco 9800 Wireless Controller and Wireless Package for Cat9K.
Affected Software version: 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
Next Step: A corrective APSP is available for 17.12.8, 17.15.6 and 17.18.4a. The corrective APSP for other IOS-XE versions (17.9.10, 26.1.2) is planned for release by Aug 15th. Cisco recommends deploying APSP once APSP is released.
Fixed Release:

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	cat9k Switches	C9350	EWC-on-9100s
17.15.6	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	Contact TAC to get Engineering Special build
17.18.4a	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA
17.18.4	NA	NA	NA	NA	NA	NA	NA	NA	APSP-Link	NA	NA
17.12.8	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA	APSP-Link	NA	Move to 17.15 train
26.1.2	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	Planned for 15th Aug	NA

17.9.10	APSP-Link	NA	APSP-Link	APSP-Link	APSP-Link	NA	NA	NA	APSP-Link	NA	Move to 17.15 train

Table 2. APSP links for different 9800 WLC platforms

CSCwv98483
Symptom: Anchored wireless clients stuck at IP_Learn when C9800-L, CW9800-L, C9800-CL are configured as foreign WLC
Affected Platforms: C9800-L, CW9800-L, C9800-CL (Only in Guest-Anchor scenario where the affected platforms act as foreign WLC)
Affected Software version: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6
Workaround: Enable Mobility Data-link encryption at the tunnel between the foreign and the anchor:

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

Fixed Release: Cisco is actively working on a fixed patch/cold SMU and customers will be notified as soon as it becomes available (Planned for release: August 21). This will be a cold SMU that requires a WLC reload.

Upgrade Guidance for Advisory and Critical Issues

To address both the advisory and critical issues reported on security hardened releases, Cisco recommends

Step 1. Wireless customers running IOS-XE version 17.12, 17.15, 17.18 proceed to Steps 2, 3 and 4. Wireless customers running IOS-XE version 17.9, 26.1, wait for APSP patch to get posted to cisco.com BEFORE upgrading. Refer to Table 2 for patch release dates

Step 2. Prior to the upgrade, run the upgrade checks and recovery steps documented here to mitigate the impact due to FN74383

Step 3. Upgrade the security hardened IOS-XE version and the APSP patch in the same maintenance window to avoid wireless service being impacted.

Step 4. If impacted by CSCwv98483, apply the workaround until SMU becomes available. Once SMU is posted, customers are expected to apply SMU patch.

Downtime Considerations for planning Maintenance Window for IOS-XE upgrade + Patches

IOS-XE upgrade on 9800 WLCs configured in non-redundant or high availability (HA) redundant configurations can leverage various mechanisms like

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

For details, refer to 9800 WLC Upgrade Quick Start Guide

In addition, the critical issues require patching with Software Maintenance Update (SMU) and Access Point Service Pack (APSP)

For details on various patching options supported by 9800 WLC, refer to Patching and Rolling AP Upgrade Guide for 9800 WLC

To plan your maintenance window for IOS-XE upgrade + patching with each upgrade mechanisms, take into account the downtime and impact documented in this section.

In-Service Software Upgrade (ISSU)

- Applicable only to 9800 WLC pair running in HA Stateful Switchover (HA SSO) configuration and only supported between long-lived release trains and their maintenance releases. (Not supported on escalation releases and short-lived release trains with no maintenance releases)
- ISSU provides seamless upgrade experience by supporting 9800 pair in HA SSO while running different software versions and leveraging rolling AP upgrade. On an operational 9800 HA pair, standby WLC is upgraded, and post SSO, new standby WLC is upgraded. For details of ISSU process and corresponding CLIs and GUI snapshots, refer to Upgrade 9800 HA SSO using ISSU
- Run the upgrade checks and recovery on APs prior to initiating ISSU.
- With ISSU, upgrade duration is not easily predictable. Depending on the size of deployment and network speeds, upgrade can take multiple "hours" to complete
- Further, ISSU leverages rolling AP upgrade where APs are rebooted in staggered fashion to minimize downtime. However, in this case, it means clients connected to APs running hardened release will continue to experience connectivity and roaming issues documented in CSCwv93265 and CSCwv98483 until WLC is patched post ISSU upgrade.
- SMU for CSCwv98483 is a cold patch that requires WLC reload.
- APSP for CSCwv93265 can be applied using Rolling AP upgrade or in one-shot. If using Rolling AP upgrade, depending on the size of the deployment, this can take several "hours" for all APs to be upgraded and definitely avoid known critical bugs
- Total duration where service might be impacted (either WLC or APs are down OR client connectivity/roaming is impacted) = Time to complete ISSU + Time for WLC reload due to SMU cold patch + Time for AP rolling upgrade for APSP

N+1 Rolling AP Upgrade

- This procedure relies on an spare 9800 WLC called as N+1 WLC with upgraded software version to host APs while "production" 9800 pair or 9800 standalone undergoes upgrade. The recommendation is for this N+1 9800 WLC to have no APs registered to it BEFORE the N+1 rolling upgrade is initiated.
- Run the upgrade checks and recovery on APs while they are registered to the primary WLC
- For details on the process and associated CLI and GUI snapshots, refer to Upgrade 9800 WLC using N+1 Rolling AP upgrade
- In this process, for APs to seamlessly roll over from primary WLC to the N+1 WLC, the software version running on N+1 WLC and predownloaded to APs needs to match exactly.
- Predownload to APs is facilitated by downloading, but NOT Activating IOS-XE hardened release on primary WLC. Without image activation, software patches cannotbe applied or predownloaded to APs. Which in turn, means N+1 WLC cannot be patched as well.
- Even in this process, like ISSU, APs rolled over to N+1 WLC will continue to be at risk for client

connectivity and roaming issues documented in CSCwv93265 and CSCwv98483 until N+1 WLC is patched, after Rolling AP upgrade finishes.

- SMU for CSCwv98483 is a cold patch that requires WLC reload.
- APSP for CSCwv93265 can be applied using Rolling AP upgrade or in one-shot. If using Rolling AP upgrade, depending on the size of the deployment, this can take several "hours" for all APs to be upgraded and definitely avoid known critical bugs
- Total duration where service might be impacted (either WLC or APs are down OR client connectivity/roaming is impacted) = Time taken for all APs to rollover to N+1 WLC + Time for WLC reload due to SMU cold patch + Time for AP rolling upgrade for APSP
- For your maintenance window, also take into account time taken for N+1 WLC to be upgraded to IOS-XE hardened releases and for APs to predownload IOS-XE hardened release from primary WLC, though neither of this will have any service impact

N+1 Regular AP Upgrade - RECOMMENDED

- This procedure relies on an spare 9800 WLC callas as N+1 WLC with upgraded software version to host APs while "production" 9800 pair or 9800 standalone undergoes upgrade.
- The recommendation is for this spare 9800 WLC to have no APs registered to it BEFORE the N+1 rolling upgrade is initiated.
- The spare N+1 WLC can be upgraded to hardened IOS-XE activated and committed and patched with APSP and SMU, in one-shot. With no APs registered, this is non-service impact but you should account for the time taken for multiple WLC reload when scheduling your maintenance window
- On the primary WLC GUI where APs are registered, navigate to COnfiguration > Tags and Profiles: AP Priming > Primary Base
    - Define N+1 WLC and Wireless Management Interface (WMI) IP Address as primary
    - Define current primary WLC name and WMI IP under Secondary
- Use regex filters to bulk migrate APs from primary WLC to N+1 WLC.
- Once registered to N+1 WLC, APs will already be running security hardened release along with patches to fix critical bugs.

Total duration where service might be impacted (either WLC or APs are down OR client connectivity/roaming is impacted) = Time taken for APs to migrate from primary WLC to N+1 WLC which is dictated by network speed between AP and WLCs.

One-Shot Upgrade - RECOMMENDED, if no N+1 WLC present

- In this procedure, the primary WLC is upgraded (along with activation and commitment) to security hardened IOS-XE release in one step.
- As part of image Activation, primary WLC gets reloaded and all APs will reregister with upgrade primary WLC and receive the security hardened IOS-XE release.
- Until APSP is applied, APs will be at risk for client connectivity and roaming issues documented in CSCwv93265 and CSCwv98483

Total duration where service might be impacted (either WLC or APs are down OR client connectivity/roaming is impacted) = Time taken for primary WLC to reload + Time taken for all APs to download hardened IOS-XE release from primary WLC over CAPWAP and register back to primary WLC. (Double this time if SMU patch is being applied) + Time taken for all APs to download APSP patch from primary WLC and register back to primary WLC.

Frequently Asked Questions

Q1. Are APs impacted by this Security Advisory?
COS based Access Points were included in the security review and the corresponding fixes are incorporated into the hardened IOS-XE releases

Q2. What is the risk for AireOS WLCs?
AireOS WLCs was not included in the security review as it has reached Last Day of Support (LDoS)