

# Correzione di IOS-XE Security Advisory - Agosto 2026 e problemi critici correlati

## Sommario

---

## Introduzione

Questo documento descrive i bug critici relativi al software wireless segnalati nelle versioni per la sicurezza avanzata pubblicate per l'advisory di IOS-XE - agosto 2026.

## Introduzione

Questo documento fornisce linee guida per l'aggiornamento per risolvere i problemi relativi a [Security Advisory](#), [FN74383](#) e i problemi critici.

Il 5 agosto 2026 Cisco ha rilasciato [IOS-XE Security Hardening Advisory](#) che ha un impatto su più piattaforme, tra cui, a titolo esemplificativo, i Wireless LAN Controller serie 9800. Come documentato, questo advisory affronta diverse vulnerabilità individuate internamente risultanti da un'analisi completa della sicurezza interna da parte di Cisco IOS-XE Engineering.

Piattaforme wireless incluse nella revisione

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

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

Embedded Wireless 9800 su switch Catalyst (9800-SW) - supporta solo l'installazione SDA

Access point Catalyst serie 11ax 91xx basato su COS  
(9105/9115/9117/9120/9130/9136/9164/9166)

Cisco Wireless serie 917x Access Point (CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

|                               |                     |
|-------------------------------|---------------------|
| Software Cisco IOS XE release | Prima release fissa |
|-------------------------------|---------------------|

|       |                    |
|-------|--------------------|
| 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             |

Tabella 1. Versioni software incluse nella revisione e corrispondenti versioni finalizzate

 \*Nota: 17.18.4a supporta tutti i WLC autonomi. Solo per il controller LAN wireless incorporato sugli switch nelle implementazioni SDA, usare il pacchetto wireless 17.18.4 che funziona con la versione 17.18.4 dello switch. Non sarà disponibile una versione 17.18.4a per lo switch o il pacchetto wireless.

## Bug critici

Nelle versioni con protezione avanzata indicate nella tabella 1, sono stati identificati alcuni problemi critici che possono influire sull'utilizzo di tali versioni.

1. [CSCwv93265](#)
2. [CSCwv98483](#)

## Dettagli dei bug critici

### [CSCwv93265](#)

Sintomo: Errori di connettività client o roaming quando sono in uso le funzionalità OpenRoaming, WPA3, 11k, 11v, 11r.

Piattaforme interessate: Tutti i controller wireless Cisco 9800 e il pacchetto wireless per Cat9K.

Versione software interessata: 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

Passaggio successivo: È disponibile un APSP correttivo per le versioni 17.12.8, 17.15.6 e 17.18.4a. La versione APSP correttiva per altre versioni di IOS-XE (17.9.10, 26.1.2) è prevista per il 15 agosto. Cisco consiglia di distribuire APSP dopo il rilascio di APSP.

Versione fissa:

|         | C9800-L                   | CW9800-L | C9800-40                  | C9800-80                  | C9800-CL                  | CW9800-M                  | CW9800-H1                 | CW9800-H2                 | Cat9k Switch              | C9350 | EWC-on-9100s                       |
|---------|---------------------------|----------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|---------------------------|-------|------------------------------------|
| 17.15.6 | <a href="#">APSP-Link</a> | N/D      | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | <a href="#">APSP-Link</a> | N/D   | Contatta TAC per ottenere la build |

|             |                              |                              |                              |                              |                              |                              |                              |                              |                              |                              |                                 |
|-------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|------------------------------|---------------------------------|
|             |                              |                              |                              |                              |                              |                              |                              |                              |                              |                              | Engineering Special             |
| 17.18.4 bis | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | N/D                          | N/D                          | N/D                             |
| 17.18.4     | N/D                          | N/D                          | N/D                          | N/D                          | N/D                          | N/D                          | N/D                          | N/D                          | <a href="#">APSP-Link</a>    | N/D                          | N/D                             |
| 17.12.8     | <a href="#">APSP-Link</a>    | N/D                          | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | N/D                          | N/D                          | N/D                          | <a href="#">APSP-Link</a>    | N/D                          | Spostarsi sul treno delle 17.15 |
| 26.1.2      | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | Pianificato per il 15 agosto | N/D                             |
| 17.9.10     | <a href="#">APSP-Link</a>    | N/D                          | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | <a href="#">APSP-Link</a>    | N/D                          | N/D                          | N/D                          | <a href="#">APSP-Link</a>    | N/D                          | Spostarsi sul treno delle 17.15 |

Tabella 2. Collegamenti APSP per diverse piattaforme 9800 WLC

#### [CSCwv98483](#)

Sintomo: Client wireless ancorati bloccati su IP\_Learn quando C9800-L, CW9800-L, C9800-CL sono configurati come WLC esterno

Piattaforme interessate: C9800-L, CW9800-L, C9800-CL (solo nello scenario Guest-Anchor in cui le piattaforme interessate fungono da WLC esterno)

Versione software interessata: Cisco IOS XE 26.1.2, Cisco IOS XE 17.18.4a, Cisco IOS XE 17.15.6

Soluzione temporanea: Abilitare la crittografia del collegamento dati di mobilità nel tunnel tra l'host esterno e l'ancoraggio:

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

Versione fissa: Cisco sta lavorando attivamente su una SMU a patch fissa/fredda e i clienti verranno informati non appena sarà disponibile (versione pianificata: 21 agosto). Si tratta di una fredda SMU che richiede un ricaricamento WLC.

## Linee guida per l'aggiornamento per i problemi critici e di consulenza

Per risolvere i problemi critici e di consulenza segnalati nelle versioni con protezione avanzata, Cisco consiglia

Passaggio 1. I clienti wireless che eseguono IOS-XE versione 17.12, 17.15, 17.18 procedono con i passaggi 2, 3 e 4. I clienti wireless che eseguono IOS-XE versione 17.9, 26.1, attendono che la patch APSP venga inviata a [cisco.com](#) PRIMA dell'aggiornamento. Per le date di rilascio delle patch, fare riferimento alla Tabella 2

Passaggio 2. Prima dell'aggiornamento, eseguire i controlli di aggiornamento e le operazioni di ripristino documentate [qui](#) per ridurre l'impatto dovuto a [FN74383](#)

Passaggio 3. Aggiornare la versione protetta di IOS-XE e la patch APSP nella stessa finestra di manutenzione per evitare che il servizio wireless venga compromesso.

Passaggio 4. Se il problema è causato da [CSCwv98483](#), applicare la soluzione alternativa finché SMU non diventa disponibile. Una volta pubblicata la SMU, i clienti devono applicare la patch SMU.

## Considerazioni sui tempi di inattività per la pianificazione della finestra di manutenzione per l'aggiornamento di IOS-XE + patch

L'aggiornamento di IOS-XE su 9800 WLC configurati in configurazioni ridondanti ad alta disponibilità (HA) o non ridondanti può utilizzare vari meccanismi, quali

- Aggiornamento software in servizio (ISSU)
- Aggiornamento in sequenza N+1
- Aggiornamento one-shot

Per ulteriori informazioni, consultare la [Guida introduttiva all'aggiornamento del WLC a 9800](#)

Inoltre, i problemi critici richiedono l'applicazione di patch con Software Maintenance Update (SMU) e Access Point Service Pack (APSP)

Per i dettagli sulle diverse opzioni di applicazione di patch supportate dal WLC 9800, fare riferimento alla [guida all'aggiornamento dell'AP in esecuzione e in sequenza per il WLC 9800](#)

Per pianificare la finestra di manutenzione per l'aggiornamento di IOS-XE + l'applicazione di patch con ciascun meccanismo di aggiornamento, tenere conto dei tempi di inattività e dell'impatto documentati in questa sezione.

### Aggiornamento software in servizio (ISSU)

- Applicabile solo a coppie WLC 9800 in esecuzione in configurazione HA Stateful Switchover (HA SSO) e supportato solo tra i treni di rilascio a lunga durata e le relative release di manutenzione. (non supportato nelle versioni con escalation e nei treni di rilascio di breve durata senza release di manutenzione)
- ISSU fornisce un'esperienza di aggiornamento senza problemi supportando coppie 9800 in

HA SSO, eseguendo diverse versioni software e sfruttando l'upgrade di rollup AP. Su una coppia 9800 HA operativa, il WLC in standby viene aggiornato e, dopo l'SSO, viene aggiornato il nuovo WLC in standby. Per informazioni dettagliate sul processo ISSU e sulle CLI e le istantanee GUI corrispondenti, consultare il documento sull'[aggiornamento 9800 HA SSO con ISSU](#)

- Eseguire i controlli di aggiornamento e il ripristino sui punti di accesso prima di avviare l'unità.
- Con IOS, la durata dell'aggiornamento non è facilmente prevedibile. A seconda delle dimensioni dell'installazione e della velocità della rete, il completamento dell'aggiornamento può richiedere più ore
- Inoltre, l'ISSU sfrutta l'upgrade in sequenza degli AP, in cui gli AP vengono riavviati in modo scaglionato per ridurre al minimo i tempi di inattività. Tuttavia, in questo caso, significa che i client connessi agli access point che eseguono una versione rinforzata continueranno a sperimentare i problemi di connettività e roaming documentati in [CSCwv93265](#) e [CSCwv98483](#) fino a quando non viene applicata una patch al WLC dopo l'aggiornamento dell'unità.
- La SMU per [CSCwv98483](#) è una patch a freddo che richiede il ricaricamento del WLC.
- APSP per [CSCwv93265](#) può essere applicato usando l'aggiornamento Rolling AP o in un'unica operazione. Se si utilizza l'aggiornamento in sequenza degli access point, a seconda delle dimensioni dell'implementazione, l'aggiornamento può richiedere diverse "ore" per tutti gli access point ed evitare definitivamente i bug critici noti
- **Durata totale in cui il servizio potrebbe essere interessato (WLC o AP inattivi O connettività/roaming client interessati) = Tempo necessario per completare l'ISSU + Tempo necessario per il ricaricamento WLC a causa della patch a freddo SMU + Tempo necessario per l'aggiornamento in sequenza AP per APSP**

## Aggiornamento punto di accesso in sequenza N+1

- Questa procedura si basa su un WLC 9800 di riserva chiamato come N+1 WLC con versione software aggiornata agli access point host, mentre la "produzione" 9800 pair o 9800 standalone viene sottoposta ad aggiornamento. Si consiglia di non registrare alcun access point per questo WLC N+1 9800 PRIMA di avviare l'aggiornamento in sequenza N+1.
- Esegui i controlli di aggiornamento e il ripristino sugli access point mentre sono registrati sul WLC primario
- Per i dettagli sul processo e le istantanee CLI e GUI associate, consultare il documento sull'[aggiornamento del WLC 9800 con l'aggiornamento del Rolling AP N+1](#)
- In questo processo, per consentire agli AP di passare senza problemi dal WLC principale al WLC N+1, la versione software in esecuzione sul WLC N+1 e prescaricata sugli AP deve corrispondere esattamente.
- Il predownload sugli access point è facilitato dal download, ma NON dall'attivazione della versione con protezione avanzata IOS-XE sul WLC primario. Senza l'attivazione dell'immagine, le patch software non possono essere applicate o prescaricate sui punti di accesso. Il che, a sua volta, significa che non è possibile applicare patch anche al WLC N+1.
- Anche in questo processo, come nel caso dell'ISSU, i punti di accesso trasferiti su WLC N+1 continueranno a essere a rischio per i problemi di connettività dei client e roaming documentati in [CSCwv93265](#) e [CSCwv98483](#) finché non verrà applicata la patch a WLC N+1, una

volta completato l'aggiornamento del punto di accesso in sequenza.

- La SMU per [CSCwv98483](#) è una patch a freddo che richiede il ricaricamento del WLC.
- APSP per [CSCwv93265](#) può essere applicato usando l'aggiornamento Rolling AP o in un'unica operazione. Se si utilizza l'aggiornamento in sequenza degli access point, a seconda delle dimensioni dell'implementazione, l'aggiornamento può richiedere diverse "ore" per tutti gli access point ed evitare definitivamente i bug critici noti
- **Durata totale in cui il servizio potrebbe essere influenzato (il WLC o gli AP sono inattivi OPPURE la connettività/il roaming dei client è influenzato) = Tempo impiegato da tutti gli AP per eseguire il rollover su N+1 WLC + Tempo impiegato per il ricaricamento del WLC a causa della patch a freddo SMU + Tempo impiegato per l'aggiornamento in sequenza dell'AP per l'APSP**
- Per la finestra di manutenzione, prendere in considerazione anche il tempo impiegato per N+1 WLC da aggiornare alle versioni con protezione avanzata IOS-XE e per gli AP per prescaricare la versione con protezione avanzata IOS-XE dal WLC principale, anche se nessuna di queste due opzioni avrà alcun impatto sul servizio

## Aggiornamento normale punto di accesso N+1 - CONSIGLIATO

- Questa procedura si basa su una chiamata 9800 WLC di riserva come N+1 WLC con versione software aggiornata agli access point dell'host, mentre la "produzione" di una coppia 9800 o standalone 9800 viene aggiornata.
- Si consiglia di non registrare alcun access point su questo WLC di riserva 9800 PRIMA di avviare l'aggiornamento in sequenza N+1.
- Il WLC di riserva N+1 può essere aggiornato a IOS-XE attivato, eseguito e dotato di patch con APSP e SMU, in un'unica operazione. Senza punti di accesso registrati, questo non ha alcun impatto sul servizio, ma è necessario tenere conto del tempo necessario per il ricaricamento di più WLC quando si pianifica la finestra di manutenzione
- Nell'interfaccia utente principale del WLC in cui sono registrati gli access point, selezionare Configurazione > Tag e profili: Priming AP > Base primaria
  - Definire l'indirizzo IP di N+1 WLC e Wireless Management Interface (WMI) come principale
  - Definire il nome WLC primario corrente e l'indirizzo IP WMI in Secondario
- Usare i filtri regex per eseguire la migrazione bulk degli AP dal WLC primario al WLC N+1.
- Una volta registrati su N+1 WLC, sugli access point sarà già in esecuzione una versione con protezione avanzata insieme alle patch per correggere i bug critici.

**Durata totale in cui il servizio potrebbe essere influenzato (il WLC o gli AP sono inattivi OPPURE la connettività/il roaming dei client è influenzato) = Tempo impiegato dagli AP per migrare dal WLC primario al WLC N+1 imposto dalla velocità di rete tra gli AP e i WLC.**

## One-Shot Upgrade - CONSIGLIATO, se non è presente alcun WLC N+1

- In questa procedura, il WLC principale viene aggiornato (insieme all'attivazione e all'impegno) alla release di IOS-XE con protezione avanzata in un unico passaggio.
- Come parte dell'attivazione dell'immagine, il WLC primario viene ricaricato e tutti gli AP si registreranno nuovamente con il WLC primario di aggiornamento e riceveranno la versione

con protezione avanzata IOS-XE.

- Fino all'applicazione dell'APSP, i punti di accesso saranno a rischio per i problemi di connettività dei client e roaming documentati in [CSCwv93265](#) e [CSCwv98483](#)

Durata totale in cui il servizio potrebbe essere influenzato (il WLC o gli AP sono inattivi O la connettività/roaming del client è influenzata) = Tempo impiegato per il ricaricamento del WLC primario + Tempo impiegato da tutti gli AP per scaricare la versione IOS-XE con protezione avanzata dal WLC primario su CAPWAP e registrarsi nuovamente sul WLC primario (raddoppiare questa durata se viene applicata la patch SMU) + Tempo impiegato da tutti gli AP per scaricare la patch APSP dal WLC primario e registrarsi nuovamente sul WLC primario.

## Domande frequenti

Q1. Questo Security Advisory ha un impatto sugli access point?

I punti di accesso basati su COS sono stati inclusi nella revisione della sicurezza e le correzioni corrispondenti sono state incorporate nelle versioni rinforzate di IOS-XE

D2. Quali sono i rischi per i WLC di AireOS?

I WLC di AireOS non sono stati inclusi nella revisione della sicurezza in quanto hanno raggiunto l'ultimo giorno di supporto (LDoS)

### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).