

修正IOS-XE安全建議 — 2026年8月及相關關鍵問題

目錄

簡介

本檔案介紹為IOS-XE建議 (2026年8月) 發佈的強化安全版本所報告的嚴重無線軟體錯誤。

背景

本文檔提供升級指南，以解決[安全建議](#)、[FN74383](#)和關鍵問題。

2026年8月5日，思科發佈了[IOS-XE安全加固建議](#)，該建議影響多個平台，包括但不限於9800系列無線LAN控制器。如前所述，此建議旨在解決因Cisco IOS-XE工程部門的全面內部安全審查而導致的多個內部發現的漏洞。

評審中包括的無線平台

Catalyst無線9800(C9800-L、C9800-CL、C9800-40、C9800-80)

Cisco無線9800 WLC(CW9800L、CW9800M、CW9800H1/H2)

Catalyst交換機(9800-SW)上的嵌入式無線9800 — 僅支援SDA部署

COS型Catalyst 11ax 91xx系列存取點(9105/9115/9117/9120/9130/9136/9164/9166)

思科無線917x系列存取點(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Cisco IOS XE軟體版本	第一個固定版本
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

表1.檢查中包含的軟體版本和相應的強化版本

 *附註:17.18.4a支援所有獨立WLC。只有在SDA部署中的交換機上的嵌入式無線LAN控制器才使用可與17.18.4交換機版本配合使用的17.18.4無線軟體包。交換機或無線軟體包沒有17.18.4a版本。

嚴重錯誤

在表1中提到的安全強化版本中，發現了一些可能會影響您對這些版本使用的關鍵問題。

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

嚴重錯誤詳細資訊

[CSCwv93265](#)

症狀：在使用OpenRoaming、WPA3、11k、11v、11r功能時，客戶端連線或漫遊失敗。

受影響的平台：適用於Cat9K的所有Cisco 9800無線控制器和無線軟體包。

受影響的軟體版本：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

下一步：糾正APSP可用於17.12.8、17.15.6和17.18.4a。其他IOS-XE版本(17.9.10、26.1.2)的修正APSP計畫在8月15日前發佈。思科建議在發佈APSP後部署APSP。

固定版本：

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	cat9k交換機	C9350	EWC-on-9100s
17.15.6	APSP-Link	不適用	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	不適用	聯絡TAC獲取工程特殊版本
17.18.4安	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	不適用	不適用	不適用
17.18.4	不適用	不適用	不適用	不適用	不適用	不適用	不適用	不適用	APSP-Link	不適用	不適用

17.12.8	APSP-Link	不適用	APSP-Link	APSP-Link	APSP-Link	不適用	不適用	不適用	APSP-Link	不適用	調到 17.15列車
26.1.2	計畫於 8月15日 發佈	計畫於8月 15日 發佈	計畫於 8月15日 發佈	計畫於 8月15日 發佈	計畫於 8月15日 發佈	計畫於8月 15日 發佈	計畫於8月 15日 發佈	計畫於8月 15日 發佈	計畫於 8月15日 發佈	計畫於 8月 15日 發佈	不適用
17.9.10	APSP-Link	不適用	APSP-Link	APSP-Link	APSP-Link	不適用	不適用	不適用	APSP-Link	不適用	調到 17.15列車

表2.適用於不同9800 WLC平台的APSP連結

[CSCwv98483](#)

症狀：當C9800-L、CW9800-L和C9800-CL配置為外部WLC時，錨定無線客戶端停滯在IP_Learn

受影響的平台：C9800-L、CW9800-L、C9800-CL（僅在受影響的平台充當外部WLC的Guest-Anchor場景中）

受影響的軟體版本：Cisco IOS XE 26.1.2、Cisco IOS XE 17.18.4a、Cisco IOS XE 17.15.6

因應措施：在外部和錨點之間的隧道上啟用移動資料鏈路加密：

```
wireless mobility group member mac-address
```

```
ip
```

```
public-ip
```

```
group
```

```
data-link-encryption
```

固定版本：思科正在積極開發固定補丁/冷SMU，一旦可用，將立即通知客戶(計畫發佈：8月21日)。這將是需要重新載入WLC的冷SMU。

諮詢問題和關鍵問題的升級指南

要解決安全強化版本中報告的顧問和關鍵問題，思科建議

步驟1. 運行IOS-XE版本17.12、17.15、17.18的無線客戶繼續執行步驟2、3和4。運行IOS-XE版本17.9、26.1的無線客戶在升級之前等待APSP補丁發佈到cisco.com。有關修補程式發行日期，請參閱表2

步驟2. 升級之前，請運行此處記錄的升級檢查和恢復[步驟](#)，以減輕由於FN而產生的[影響74383](#)

步驟3. 在同一維護視窗中升級經過安全強化的IOS-XE版本和APSP補丁以避免無線服務受到影響。

步驟4. 如果受[CSCwv98483](#)影響，請[應用解決方法](#)，直到SMU可用。一旦SMU發佈，客戶需要應用SMU補丁程式。

規劃IOS-XE升級維護視窗時的停機注意事項+修補程式

以非備援或高可用性(HA)備援設定的9800 WLC上的IOS-XE升級可利用各種機制，例如

- 服務中軟體升級(ISSU)
- N+1滾動升級
- 一次性升級

有關詳細資訊，請參閱[9800 WLC升級快速入門手冊](#)

此外，關鍵問題需要使用軟體維護更新(SMU)和接入點服務包(APSP)進行修補

有關9800 WLC支援的各種修補選項的詳細資訊，請參閱[9800 WLC的修補和滾動AP升級指南](#)

要使用每個升級機制規劃IOS-XE升級和修補的維護視窗，請考慮本節中記錄的停機時間和影響。

服務中軟體升級(ISSU)

- 僅適用於在HA狀態切換(HA SSO)設定中執行的9800 WLC配對，且僅適用於長壽命版本系列與其維護版本之間受支援。(升級版本和沒有維護版本的短期版本系列不支援)
- ISSU通過支援HA SSO中的9800對，同時運行不同的軟體版本並利用滾動的AP升級，提供了無縫的升級體驗。在可操作的9800 HA配對上，待命WLC會升級，且在SSO之後，新的待命WLC會升級。有關ISSU過程和相應的CLI和GUI快照的詳細資訊，請參閱[使用ISSU升級9800 HA SSO](#)
- 在啟動ISSU之前，在AP上運行升級檢查和恢復。
- 使用ISSU時，升級持續時間不易預測。根據部署規模和網路速度，完成升級可能需要數小時

- 此外，ISSU利用逐段重新啟動AP的滾動式接入點升級，以最大限度地減少停機時間。但是在這種情況下，這意味著連線到運行強化版本AP的客戶端在ISSU升級後修補WLC之前，將繼續遇到記錄在[CSCwv93265](#)和[CSCwv98483](#)中的連線和漫遊問題。
- [CSCwv98483](#)的SMU是一個冷補丁，需要WLC重新載入。
- 適用於[CSCwv93265](#)的APSP可以使用滾動AP升級或一次性應用。如果使用滾動式AP升級，則升級所有AP可能需要幾個「小時」，這取決於部署的大小，並且肯定能夠避免已知的關鍵錯誤
- 服務可能受到影響的總持續時間 (WLC或AP關閉或客戶端連線/漫遊受到影響) =完成ISSU的時間+由於SMU冷補丁而導致WLC重新載入的時間+APSP的AP滾動升級時間

N+1滾動AP升級

- 此過程依賴於名為N+1 WLC的備件9800 WLC，其軟體版本已升級為主機AP，而「production」9800對或9800獨立版正在升級。建議在N+1滾動升級啟動之前，此N+1 9800 WLC沒有向其註冊AP。
- 將AP註冊到主WLC時，對AP運行升級檢查和恢復
- 有關過程以及相關CLI和GUI快照的詳細資訊，請參閱[使用N+1滾動AP升級升級9800 WLC](#)
- 在此過程中，要將AP從主WLC無縫地滾動到N+1 WLC，N+1 WLC上運行並預先下載到AP的軟體版本需要完全匹配。
- 下載但不啟用主WLC上的IOS-XE強化版有助於預下載到AP。如果沒有映像啟用，則無法向AP應用或預下載軟體修補程式。這進而意味著N+1 WLC也不能進行修補。
- 即使在此過程中，與ISSU一樣，在累積AP升級完成後，滾動到N+1 WLC的AP仍會面臨客戶端連線和漫遊問題(記錄在[CSCwv93265](#)和[CSCwv98483](#)中)。
- [CSCwv98483](#)的SMU是一個冷補丁，需要WLC重新載入。
- 適用於[CSCwv93265](#)的APSP可以使用滾動AP升級或一次性應用。如果使用滾動式AP升級，則升級所有AP可能需要幾個「小時」，這取決於部署的大小，並且肯定能夠避免已知的關鍵錯誤
- 可能影響服務的總持續時間 (WLC或AP關閉或客戶端連線/漫遊受到影響) =所有AP滾動到N+1 WLC所用的時間+因SMU冷補丁而導致WLC重新載入的時間+APSP的AP滾動升級所用的時間
- 在維護時段中，還應考慮N+1 WLC升級到IOS-XE強化版本以及AP從主WLC預下載IOS-XE強化版本所用的時間，儘管這兩種操作都不會對服務產生任何影響

N+1常規AP升級 — 推薦

- 此程式依賴於備件9800 WLC呼叫 (即N+1 WLC)，其軟體版本已升級為主機AP，而「production」9800對或9800獨立版正在進行升級。
- 建議在N+1滾動升級啟動之前，此備件9800 WLC沒有註冊到它的AP。
- 一次即可將備用N+1 WLC升級為強化的IOS-XE啟用和提交，並使用APSP和SMU進行修補。如果沒有註冊AP，則不會產生服務影響，但您應在計畫維護時段時考慮多次WLC重新載入所用的時間
- 在註冊AP的主WLC GUI上，導航至Configuration > Tags and Profiles:AP預備>主要基礎
 - 將N+1 WLC和無線管理介面(WMI)IP地址定義為主地址
 - 在Secondary下定義當前主WLC名稱和WMI IP
- 使用regex過濾器將AP從主WLC批次遷移到N+1 WLC。
- 註冊到N+1 WLC後，AP將運行經過安全強化處理的版本，以及修復關鍵錯誤的補丁。

可能影響服務的總持續時間 (WLC或AP關閉或客戶端連線/漫遊受到影響) = AP從主WLC遷移到N+1 WLC所用的時間，由AP和WLC之間的網路速度決定。

一次性升級 — 如果沒有N+1 WLC，則建議使用

- 在此過程中，系統會一步將主WLC升級 (以及啟用和承諾) 到經過安全強化的IOS-XE版本。
- 作為映像啟用的一部分，主WLC會重新載入，所有AP將通過升級主WLC重新註冊並接收經過安全強化的IOS-XE版本。
- 在應用APSP之前，AP可能會面臨客戶端連線和漫遊問題，CSCwv93265和[CSCwv98483](#)中有相關記錄

服務可能受到影響 (WLC或AP關閉或客戶端連線/漫遊受到影響) 的總持續時間=主WLC重新載入所用的時間+所有AP通過CAPWAP從主WLC下載強化的IOS-XE版本並註冊回主WLC所用的時間。(如果正在應用SMU補丁，則此時間加倍) +所有AP從主WLC下載APSP補丁並註冊回主WLC所用的時間。

常見問題

問題1.此安全顧問是否會影響AP？

基於COS的接入點已包括在安全審查中，相應的修復已整合到強化的IOS-XE版本中

問題2. AireOS WLC有哪些風險？

AireOS WLC未包括在安全檢查中，因為它已達到最後支援日(LDoS)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。