

修复IOS-XE安全建议 — 2026年8月及相关关键问题

目录

简介

本文档介绍针对IOS-XE建议 (2026年8月) 发布的强化安全版本所报告的严重无线软件漏洞。

背景

本文档提供升级指南，以解决[安全建议](#)、[FN74383](#)和关键问题。

2026年8月5日，思科发布了[IOS-XE安全强化建议](#)，该建议会影响多个平台，包括但不限于9800系列无线局域网控制器。如前所述，此建议解决了由Cisco IOS-XE工程部门进行全面的内部安全审核后在内部发现的多个漏洞。

审核中包括的无线平台

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

思科无线9800 WLC(CW9800L、CW9800M、CW9800H1/H2)

Catalyst交换机(9800-SW)上的嵌入式无线9800 — 仅支持SDA部署

基于COS的Catalyst 11ax 91xx系列接入点(9105/9115/9117/9120/9130/9136/9164/9166)

思科无线917x系列接入点(CW9171/CW9172/CW9174/CW9176/CW9178/CW9179)

Cisco IOS XE软件版本	第一个固定版本
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.审查中包含的软件版本和相应的强化版本

 *注:17.18.4a支持所有独立WLC。只有在SDA部署中的交换机上使用嵌入式无线局域网控制器，才能使用与17.18.4交换机版本配合使用的17.18.4无线软件包。交换机或无线软件包没有17.18.4a版本。

严重错误

在表1中提到的安全强化版中，发现了一些可能会影响您使用这些版本的关键问题。

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

严重漏洞详细信息

[CSCwv93265](#)

症状：使用OpenRoaming、WPA3、11k、11v、11r功能时的客户端连接或漫游故障。

受影响的平台：适用于Cat9K的所有Cisco 9800无线控制器和无线软件包。

受影响的软件版本：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：纠正APSP可用于17.12.8、17.15.6和17.18.4a。其他IOS-XE版本(17.9.10、26.1.2)的更正APSP计划在8月15日发布。思科建议在APSP发布后部署APSP。

固定版本：

	C9800-L	CW9800-L	C9800-40	C9800-80	C9800-CL	CW9800-M	CW9800-H1	CW9800-H2	cat9k交换机	C9350	EWC-on-9100s
17.15.6	APSP-Link	不适用	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	不适用	联系TAC获取工程专业版本
17.18.4安	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	APSP-Link	不适用	不适用	不适用
17.18.4	不适用	不适用	不适用	不适用	不适用	不适用	不适用	不适用	APSP-Link	不适用	不适用

17.12.8	APSP-Link	不适用	APSP-Link	APSP-Link	APSP-Link	不适用	不适用	不适用	APSP-Link	不适用	调到17.15列车
26.1.2	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	计划于8月15日发布	不适用
17.9.10	APSP-Link	不适用	APSP-Link	APSP-Link	APSP-Link	不适用	不适用	不适用	APSP-Link	不适用	调到17.15列车

表2.适用于不同9800 WLC平台的APSP链路

[CSCwv98483](#)

症状：当C9800-L、CW9800-L、C9800-CL配置为外部WLC时，锚定无线客户端停滞在IP_Learn

受影响的平台：C9800-L、CW9800-L、C9800-CL (仅在受影响的平台用作外部WLC的Guest-Anchor场景中)

受影响的软件版本：Cisco IOS XE 26.1.2、Cisco IOS XE 17.18.4a、Cisco IOS XE 17.15.6

解决方法：在外部和锚点之间的隧道上启用移动数据链路加密：

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

```
ip
```

```
public-ip
```

```
group
```

```
data-link-encryption
```

固定版本：思科正在积极开发固定补丁/冷SMU，一旦可用，客户就会收到通知(计划发布：8月21日)。这将是需要WLC重新加载的冷SMU。

咨询问题和关键问题的升级指南

为解决安全强化版本中报告的咨询问题和关键问题，思科建议

步骤1.运行IOS-XE版本17.12、17.15、17.18的无线客户继续步骤2、3和4。运行IOS-XE版本17.9、26.1的无线客户在升级之前等待APSP补丁发布到cisco.com。有关补丁发布日期，请参阅表2

步骤2.在升级之前，请运行此处记录的升级检查和恢复[步骤](#)，以减轻由于FN而产生的[影响74383](#)

步骤3.在同一维护窗口中升级经过安全强化的IOS-XE版本和APSP补丁以避免无线服务受到影响。

第4步：如果受到[CSCwv98483的影响](#)，请应用解决方法，直到SMU可用为止。发布SMU后，客户需要应用SMU补丁。

规划IOS-XE升级维护窗口时的停机注意事项+补丁

在非冗余或高可用性(HA)冗余配置下配置的9800 WLC上的IOS-XE升级可以利用各种机制，例如

- 服务中软件升级(ISSU)
- N+1滚动升级
- 一次性升级

有关详细信息，请参阅[9800 WLC升级快速入门指南](#)

此外，关键问题需要使用软件维护更新(SMU)和接入点服务包(APSP)进行修补

有关9800 WLC支持的各种修补选项的详细信息，请参阅[9800 WLC的修补和滚动AP升级指南](#)

要为每个升级机制规划IOS-XE升级和修补的维护窗口，请考虑本节中记录的停机时间和影响。

服务中软件升级(ISSU)

- 仅适用于在HA状态切换(HA SSO)配置中运行的9800 WLC对，并且仅在长寿命版本系列及其维护版本之间受支持。（升级版本和不带维护版本的短期版本系列不支持）
- ISSU通过支持HA SSO中的9800对，同时运行不同的软件版本，并利用滚动式AP升级，提供无缝的升级体验。在运行中的9800 HA对上，升级备用WLC，并且在SSO之后，升级新的备用WLC。有关ISSU过程和相应的CLI和GUI快照的详细信息，请参阅[使用ISSU升级9800 HA SSO](#)
- 在启动ISSU之前，在AP上运行升级检查和恢复。
- 使用ISSU时，升级持续时间不容易预测。根据部署规模和网络速度，完成升级可能需要数小

时

- 此外，ISSU利用轮循AP升级，AP以交错方式重新启动，以最大限度地减少停机时间。但是，在本例中，这意味着连接到运行强化版本的AP的客户端在ISSU升级后修复WLC之前，将继续遇到记录在[CSCwv93265](#)和[CSCwv98483](#)中的连接和漫游问题。
- [CSCwv98483](#)的SMU是需要WLC重新加载的冷补丁。
- 适用于[CSCwv93265](#)的APSP可使用滚动式AP升级或一次性应用。如果使用滚动AP升级，则升级所有AP可能需要几个“小时”，这取决于部署的大小，并且肯定能避免已知的严重漏洞
- 可能影响服务的总持续时间（WLC或AP关闭或客户端连接/漫游受到影响）=完成ISSU的时间+由于SMU冷补丁而导致WLC重新加载的时间+APSP的AP滚动升级时间

N+1滚动AP升级

- 此过程依赖于名为N+1 WLC的备件9800 WLC，它升级了主机AP的软件版本，而“生产”的9800对或9800独立版进行升级。建议在N+1滚动升级启动之前，此N+1 9800 WLC没有向其注册AP。
- 当AP注册到主WLC时，在它们上运行升级检查和恢复
- 有关流程和相关的CLI和GUI快照的详细信息，请参阅[使用N+1滚动AP升级升级9800 WLC](#)
- 在此过程中，为了使AP从主WLC无缝滚动到N+1 WLC，N+1 WLC上运行并预下载到AP的软件版本需要完全匹配。
- 通过下载而不是激活主WLC上的IOS-XE强化版本可以方便地预下载到AP。如果没有映像激活，则无法向AP应用或预下载软件补丁。这又意味着N+1 WLC也无法修补。
- 即使在此过程中，与ISSU一样，滚动到N+1 WLC的AP仍会面临客户端连接和漫游问题（记录在[CSCwv93265](#)和[CSCwv98483](#)中），直到滚动的AP升级完成后N+1 WLC得到修补。
- [CSCwv98483](#)的SMU是需要WLC重新加载的冷补丁。
- 适用于[CSCwv93265](#)的APSP可使用滚动式AP升级或一次性应用。如果使用滚动AP升级，则升级所有AP可能需要几个“小时”，这取决于部署的大小，并且肯定能避免已知的严重漏洞
- 服务可能受到影响的总持续时间（WLC或AP关闭或客户端连接/漫游受到影响）=所有AP滚动到N+1 WLC所用的时间+由于SMU冷补丁而导致WLC重新加载的时间+APSP滚动升级AP所用的时间
- 在维护时段中，还要考虑N+1 WLC升级至IOS-XE强化版本和AP从主WLC预下载IOS-XE强化版本所花费的时间，尽管这两种操作都不会对服务造成任何影响

N+1常规AP升级 — 推荐

- 此过程依赖于作为N+1 WLC的备用9800 WLC呼叫，该呼叫具有升级的软件版本以托管接入点，而“production”9800对或9800独立交换机正在进行升级。
- 建议此备用9800 WLC在启动N+1滚动升级之前不向其注册AP。
- 备用N+1 WLC可一次性升级到强化的IOS-XE激活和提交，并使用APSP和SMU进行修补。如果未注册AP，这不会影响服务，但您应在计划维护窗口时考虑多次WLC重新加载所花费的时间
- 在注册AP的主要WLC GUI上，导航到Configuration > Tags and Profiles:AP初始化>主基础
 - 将N+1 WLC和无线管理接口(WMI)IP地址定义为主要地址
 - 在Secondary下定义当前主WLC名称和WMI IP
- 使用regex过滤器将AP从主WLC批量迁移到N+1 WLC。

- 注册到N+1 WLC后，AP将运行经过安全强化处理的版本以及修复关键错误的补丁。

可能影响服务的总持续时间（WLC或AP关闭或客户端连接/漫游受到影响）=AP从主WLC迁移到N+1 WLC所用的时间，由AP和WLC之间的网络速度决定。

一次性升级 — 如果没有N+1 WLC，则建议进行升级

- 在此程序中，主WLC在一个步骤中升级（连同激活和承诺）到经过安全强化的IOS-XE版本。
- 作为映像激活的一部分，主WLC重新加载，所有AP将通过升级主WLC重新注册并接收经过安全强化的IOS-XE版本。
- 在应用APSP之前，AP将面临记录在[CSCwv93265](#)和[CSCwv98483](#)中的客户端连接和漫游问题的[风险](#)

服务可能受到影响（WLC或AP关闭或客户端连接/漫游受到影响）的总持续时间=主WLC重新加载所用的时间+所有AP通过CAPWAP从主WLC下载强化的IOS-XE版本并注册回主WLC所用的时间。（如果应用SMU补丁，则此时间加倍）+所有AP从主WLC下载APSP补丁并注册回主WLC所用的时间。

常见问题解答

问题1:AP是否受此安全建议的影响？

基于COS的接入点已包括在安全审核中，相应的修复已整合到强化的IOS-XE版本中

问题2. AireOS WLC有哪些风险？

AireOS WLC未包括在安全审核中，因为它已达到最后支持日(LDoS)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。