Cisco Security Advisory

Cisco IOS XE Wireless Controller Software Cisco Discovery Protocol Denial of Service Vulnerability

High

Advisory ID:
cisco-sa-ewlc-cdp-dos-fpeks9K

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwm14282

CVE-2025-20202

CWE-805

CVSS Score:
Base 7.4

Download CSAF Email

Summary

A vulnerability in Cisco IOS XE Wireless Controller Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device.

This vulnerability is due to insufficient input validation of access point (AP) Cisco Discovery Protocol (CDP) neighbor reports when they are processed by the wireless controller. An attacker could exploit this vulnerability by sending a crafted CDP packet to an AP. A successful exploit could allow the attacker to cause an unexpected reload of the wireless controller that is managing the AP, resulting in a DoS condition that affects the wireless network.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-cdp-dos-fpeks9K

This advisory is part of the May 2025 release of the Cisco IOS and IOS XE Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see Cisco Event Response: May 2025 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication.

Affected Products

Vulnerable Products

This vulnerability affects the following Cisco products if they are running a vulnerable release of Cisco IOS XE Software and have AP CDP enabled:

- Catalyst 9800-CL Wireless Controllers for Cloud
- Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches
- Catalyst 9800 Series Wireless Controllers
- Embedded Wireless Controllers on Catalyst APs

For information about which Cisco software releases are vulnerable, see the Fixed Software section of this advisory.

Determine the Device Configuration

A device is affected by this vulnerability when CDP is enabled for any APs that are managed by the device. CDP is enabled by default and can be configured from the AP Join profile section on the wireless controller.

To determine if a device is affected, a user with *Administrator* privileges can connect to the device CLI and issue the **show running-config | section ap profile** command. If the output for every AP Join profile that is configured on the device contains the line **no cdp**, then the device is not affected. If the output for at least one AP Join profile does not contain this line, then CDP is enabled for all APs under that AP Join profile, and the device is affected.

In the following example, **new-ap-profile** has CDP disabled, but **default-ap-profile** has CDP enabled. Therefore, the device is affected.

```
WLC#show running-config | section ap profile
ap profile new-ap-profile
 no cdp
 ntp ip 0.0.0.0
 syslog host 255.255.255.255
ap profile default-ap-profile
 description "default ap profile"
 ntp ip 0.0.0.0
 syslog host 255.255.255.255
```

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to be affected by this vulnerability.

Cisco has confirmed that this vulnerability does not affect the following Cisco products:

- IOS Software
- IOS XR Software
- Meraki products
- NX-OS Software
- Wireless LAN Controller (WLC) AireOS Software

Workarounds

There are no workarounds that address this vulnerability.

However, if CDP is not required on the AP, an administrator can disable CDP on every AP profile from either the web-based management GUI or CLI.

Disable AP CDP from the Web-Based Management GUI

To disable the AP CDP from the web-based management GUI, use the following steps:

1. Choose **Configuration > Tags & Profiles > AP Join**.
2. For every AP profile that is configured on the device, click the profile name, then choose **Management > CDP Interface**.
3. Set the **CDP State** to **Disabled**.

Disable AP CDP from the Management CLI

To disable the AP CDP from the management CLI on the wireless controller, use the following steps:

1. Confirm the AP profile names using the **show ap ap-join-profile summary** command, as shown in the following example:

```
WLC#show ap ap-join-profile summary


Number of AP Profiles: 2
AP Profile Name                  Description
------------------------------------------------------------------------
new-ap-profile
default-ap-profile               default ap profile
```

2. Enter configuration mode. For every AP Join profile, enter the **no cdp** command, as shown in the following example:

```
WLC#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
WLC(config)#ap profile new-ap-profile
WLC(config-ap-profile)#no cdp
WLC(config-ap-profile)#ap profile default-ap-profile
WLC(config-ap-profile)#no cdp
WLC(config-ap-profile)#end
```

To verify the configuration, see the instructions in the Vulnerable Products section of this advisory.

While this mitigation has been deployed and was proven successful in a test environment, customers should determine the applicability and effectiveness in their own environment and under their own use conditions. Customers should be aware that any workaround or mitigation that is implemented may negatively impact the functionality or performance of their network based on intrinsic customer deployment scenarios and limitations. Customers should not deploy any workarounds or mitigations before first evaluating the applicability to their own environment and any impact to such environment.

Fixed Software

Cisco has released free software updates that address the vulnerability described in this advisory. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

Customers may only install and expect support for software versions and feature sets for which they have purchased a license. By installing, downloading, accessing, or otherwise using such software upgrades, customers agree to follow the terms of the Cisco software license: https://www.cisco.com/c/en/us/products/end-user-license-agreement.html

Additionally, customers may only download software for which they have a valid license, procured from Cisco directly, or through a Cisco authorized reseller or partner. In most cases this will be a maintenance upgrade to software that was previously purchased. Free security software updates do not entitle customers to a new software license, additional software feature sets, or major revision upgrades.

The Cisco Support and Downloads page on Cisco.com provides information about licensing and downloads. This page can also display customer device support coverage for customers who use the My Devices tool.

When considering software upgrades, customers are advised to regularly consult the advisories for Cisco products, which are available from the Cisco Security Advisories page, to determine exposure and a complete upgrade solution.

In all cases, customers should ensure that the devices to be upgraded contain sufficient memory and confirm that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, customers are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

Customers Without Service Contracts

Customers who purchase directly from Cisco but do not hold a Cisco service contract and customers who make purchases through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should obtain upgrades by contacting the Cisco TAC: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Customers should have the product serial number available and be prepared to provide the URL of this advisory as evidence of entitlement to a free upgrade.

Cisco IOS and IOS XE Software

To help customers determine their exposure to vulnerabilities in Cisco IOS and IOS XE Software, Cisco provides the Cisco Software Checker. This tool identifies any Cisco security advisories that impact a specific software release and the earliest release that fixes the vulnerabilities that are described in each advisory (“First Fixed”). If applicable, the tool also returns the earliest release that fixes all the vulnerabilities that are described in all the advisories that the Software Checker identifies (“Combined First Fixed”).

To use the tool, go to the Cisco Software Checker page and follow the instructions. Alternatively, use the following form to determine whether a release is affected by any Cisco Security Advisory. To use the form, follow these steps:

1. Choose which advisories the tool will search–only this advisory, only advisories with a Critical or High Security Impact Rating (SIR), or all advisories.
2. Enter a release number–for example, 15.9(3)M2 or 17.3.3.
3. Click **Check**.

Only this advisory

Enter release number Check

Exploitation and Public Announcements

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Source

This vulnerability was found during the resolution of a Cisco TAC support case.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-cdp-dos-fpeks9K

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-MAY-07

Legal Disclaimer

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Your Rating:

Average Rating:

5 star	0
4 star	0
3 star	0
2 star	0
1 star	0

Leave additional feedback