Cisco Security Advisory

# Cisco IOS XE Software for WLC Wireless IPv6 Clients Denial of Service Vulnerability

High

Advisory ID:
cisco-sa-wlc-wncd-p6Gvt6HL

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwj16556

CVE-2025-20140

CWE-789

CVSS Score:
Base 7.4

Download CSAF Email

## Summary

A vulnerability in the Wireless Network Control daemon (wncd) of Cisco IOS XE Software for Wireless LAN Controllers (WLCs) could allow an unauthenticated, adjacent wireless attacker to cause a denial of service (DoS) condition.

This vulnerability is due to improper memory management. An attacker could exploit this vulnerability by sending a series of IPv6 network requests from an associated wireless IPv6 client to an affected device. To associate a client to a device, an attacker may first need to authenticate to the network, or associate freely in the case of a configured open network. A successful exploit could allow the attacker to cause the wncd process to consume available memory and eventually cause the device to stop responding, resulting in a DoS condition.

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-wlc-wncd-p6Gvt6HL

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 for WLCs with support enabled for wireless IPv6 clients:

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

**Note:** Support for wireless IPv6 clients is enabled by default on Cisco IOS XE Software for WLCs.

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

#### Determine the Device Configuration

To determine whether the device supports IPv6 wireless clients, use the **show run all | include wireless\ ipv6\ client** command. If the command returns **wireless ipv6 client**, the device supports IPv6 clients and may be affected by this vulnerability, as shown in the following example:

```
9800#show run all | include wireless\ ipv6\ client
wireless ipv6 client
```

### Products Confirmed Not Vulnerable

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

- IOS Software
- IOS XR Software
- Meraki products
- NX-OS Software
- WLC AireOS Software

## Workarounds

There are no workarounds that address this vulnerability.

However, customers can disable wireless IPv6 clients by issuing the **no wireless ipv6 client** command if the feature is not in use.

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-wlc-wncd-p6Gvt6HL

## 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

About Cisco

Contact Us

Careers

Connect with a partner

## Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap