Cisco Security Advisory

Cisco IOS XE Wireless Controller Software Unauthorized User Deletion Vulnerability

Medium

Advisory ID:
cisco-sa-ewlc-user-del-hQxMpUDj

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwm35433

CVE-2025-20190

CWE-284

CVSS Score:
Base 6.5

Download CSAF Email

Summary

A vulnerability in the lobby ambassador web interface of Cisco IOS XE Wireless Controller Software could allow an authenticated, remote attacker to remove arbitrary users that are defined on an affected device.

This vulnerability is due to insufficient access control of actions executed by lobby ambassador users. An attacker could exploit this vulnerability by logging in to an affected device with a *lobby ambassador* user account and sending crafted HTTP requests to the API. A successful exploit could allow the attacker to delete arbitrary user accounts on the device, including users with administrative privileges.

Note: This vulnerability is exploitable only if the attacker obtains the credentials for a *lobby ambassador* account. This account is not configured by default.

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-user-del-hQxMpUDj

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

At the time of publication, this vulnerability affected the following Cisco products if they were running a vulnerable release of Cisco IOS XE Wireless Controller Software and had *lobby ambassador* user accounts 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 Access Points

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory.

Determine the Device Configuration

To determine whether a *lobby ambassador* account and the HTTP server feature are configured on a device, use the following instructions.

Determine the Lobby Ambassador Account Configuration

To determine how many *lobby ambassador* accounts are configured on a device, log in to the device and run the **show running-config | count type lobby-admin** CLI command. The following example shows the CLI output on a device with one *lobby ambassador* account configured:

```
Router#show running-config | count type lobby-admin
Number of lines which match regexp = 1
```

The number at the end of the line indicates how many *lobby ambassador* accounts are configured on the device.

Note: The lobby ambassador role can be associated with a user account that is using RADIUS or TACACS+. Customers who are using an authentication, authorization, and accounting (AAA) server such as Cisco Identity Services Engine (ISE) to manage user accounts that are accessing their device should check for the presence of users that have the cisco-av-pair=lobby-admin attribute set. For an example of how to configure a *lobby ambassador* account on Cisco ISE, see Configure 9800 WLC Lobby Ambassador with RADIUS and TACACS+ Authentication.

Determine the HTTP Server Configuration

To determine whether the HTTP Server feature is enabled for a device, log in to the device and use the **show running-config | include ip http server|secure|active** command in the CLI to check for the presence of the **ip http server** command or the **ip http secure-server** command in the global configuration. If either command is present, the HTTP Server feature is enabled for the device.

The following example shows the output of the **show running-config | include ip http server|secure|active** command for a device that has the HTTP Server feature enabled:

```
Router# show running-config | include ip http server|secure|active
ip http server
ip http secure-server
```

Note: The presence of either command or both commands in the device configuration indicates that the web UI feature is enabled.

If the **ip http server** command is present and the configuration also contains **ip http active-session-modules none**, the vulnerability is not exploitable over HTTP.

If the **ip http secure-server** command is present and the configuration also contains **ip http secure-active-session-modules none**, the vulnerability is not exploitable over HTTPS.

Cisco IOS XE Wireless Controller Software is affected by this vulnerability only if the device is configured with a *lobby ambassador* account. This is not a default configuration and must be added by an administrator.

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.

Fixed Software

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.

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 internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-user-del-hQxMpUDj

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

Quick Links

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