Cisco Security Advisory

Cisco IOS XE Software Web-Based Management Interface Vulnerabilities

Medium

Advisory ID:
cisco-sa-webui-multi-ARNHM4v6

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwk16979 , CSCwk23580 , CSCwk25133

CVE-2025-20193

CVE-2025-20194

CVE-2025-20195

CWE-352

CWE-78

CVSS Score:
Base 6.5

Download CSAF Email

Summary

Multiple vulnerabilities in the web-based management interface of Cisco IOS XE Software could allow a remote attacker to read files from the underlying operating system, read limited parts of the configuration file, clear the syslog, or conduct a cross-site request forgery (CSRF) attack on an affected device, depending on their privilege level.

For more information about these vulnerabilities, see the Details section of this advisory.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-multi-ARNHM4v6

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, these vulnerabilities affected Cisco IOS XE Software if it had the web-based management interface enabled.

Note: To enable the web-based management interface, use the **ip http server** or **ip http secure-server** command.

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

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-based management interface 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.

Products Confirmed Not Vulnerable

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

Cisco has confirmed that these vulnerabilities do not affect the following Cisco products:

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

Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerabilities.

Details about the vulnerabilities are as follows:

CVE-2025-20193: Cisco IOS XE Software Information Disclosure Vulnerability

A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, low-privileged, remote attacker to perform an injection attack against an affected device.

This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to read files from the underlying operating system.

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

Bug ID(s): CSCwk16979
CVE ID: CVE-2025-20193
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

CVE-2025-20194: Cisco IOS XE Software Command Injection Vulnerability

A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an authenticated, low-privileged, remote attacker to perform an injection attack against an affected device.

This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web-based management interface. A successful exploit could allow the attacker to read limited files from the underlying operating system or clear the syslog and licensing logs on the affected device.

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

Bug ID(s): CSCwk25133
CVE ID: CVE-2025-20194
Security Impact Rating (SIR): Medium
CVSS Base Score: 5.4
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVE-2025-20195: Cisco IOS XE Software Web-Based Management Interface CSRF Vulnerability

A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a CSRF attack and execute commands on the CLI of an affected device.

This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an already authenticated user to follow a crafted link. A successful exploit could allow the attacker to clear the syslog, parser, and licensing logs on the affected device if the targeted user has privileges to clear those logs.

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

Bug ID(s): CSCwk23580
CVE ID: CVE-2025-20195
Security Impact Rating (SIR): Medium

CVSS Base Score: 4.3
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Workarounds

There are no workarounds that address these vulnerabilities.

Disabling the HTTP Server feature eliminates the attack vector for these vulnerabilities and may be a suitable mitigation until affected devices can be upgraded. To disable the HTTP Server feature, use the **no ip http server** or **no ip http secure-server** command in global configuration mode. If both the HTTP server and HTTPS server are in use, both commands are required to disable the HTTP Server feature.

Allowing only trusted networks to access the HTTP server will limit exposure to these vulnerabilities. The following example shows how to allow remote access to the HTTP server from the trusted *192.168.10.0/24* network:

```
!
ip http access-class ipv4 restrict_ipv4_webui
!
ip access-list standard restrict_ipv4_webui
permit 192.168.10.0 0.0.0.255
!
```

For additional information, see Filter Traffic Destined to Cisco IOS XE Devices WebUI Using an Access List.

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

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 vulnerabilities that are described in this advisory.

Source

These vulnerabilities were found during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-multi-ARNHM4v6

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