Cisco Security Advisory

Cisco IOx Application Hosting Environment Denial of Service Vulnerability

Medium

Advisory ID:
cisco-sa-iox-dos-95Fqnf7b

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwj81278

CVE-2025-20196

CWE-307

CVSS Score:
Base 5.3

Download CSAF Email

Summary

A vulnerability in the Cisco IOx application hosting environment of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the Cisco IOx application hosting environment to stop responding, resulting in a denial of service (DoS) condition.

This vulnerability is due to the improper handling of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to cause the Cisco IOx application hosting environment to stop responding. The IOx process will need to be manually restarted to recover services.

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-iox-dos-95Fqnf7b

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 Cisco IOS and IOS XE Software if they were configured with the Cisco IOx application hosting environment and have the HTTP Server feature enabled. The Cisco IOx application hosting environment is not enabled by default.

At the time of publication, this vulnerability also affected the following Cisco products:

- 800 Series Industrial ISRs
- Catalyst 9100 Family of Access Points (COS-AP)
- CGR1000 Compute Modules
- IC3000 Industrial Compute Gateways
- IR510 WPAN Industrial Routers

For information about which Cisco software releases were vulnerable at the time of publication, see the Fixed Software section of this advisory. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

Determine Whether the IOx Application Hosting Environment Is Enabled

Option 1: Use the **show iox-service** CLI command.

To determine the status of IOx functionality, use the **show iox-service** command in privileged EXEC mode, as shown in the following example:

```
Router#show iox-service
IOx Infrastructure Summary:
---------------------------
IOx service (CAF)          : Running
IOx service (HA)           : Running
IOx service (IOxman)       : Running
Libvirtd                   : Running
```

If **IOx service (CAF)** is in **Running** state, the device may be affected by this vulnerability. Proceed to Determine the HTTP Server Configuration.

If any of the following statements is true, the device is not affected by this vulnerability:

- **IOx service (CAF)** is in **Not Running** state.
- The **show iox-service** privileged EXEC mode command returns no output.
- The **show iox-service** privileged EXEC mode command returns an error.

Option 2: Use the **iox** configuration command.

As an alternative, check the running configuration for the **iox** configuration command, as shown in the following example:

```
Router#sh run | include iox
iox
```

If the output contains a line with only **iox**, as shown in the example, the device may be affected by this vulnerability. Proceed to Determine the HTTP Server Configuration.

If the **iox** configuration command does not return output or returns an error, the device is not affected by this vulnerability.

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.

Restore the IOx Application Environment

The Cisco IOx application hosting environment will not recover without user intervention. It must be restarted with the **no iox** and then **iox** configuration commands, as shown in the following example:

```
Router(config)# no iox
Router(config)# iox
```

Products Confirmed Not Vulnerable

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

Workarounds

There are no workarounds that address this vulnerability.

However, there is a mitigation. Cisco recommends that customers who do not require the Cisco IOx application hosting environment disable Cisco IOx on the device using the **no iox** configuration command. If the Cisco IOx hosting environment is required, the HTTP server can be disabled with the **no ip http server** and **no ip http secure-server** configuration commands.

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.

Fixed Releases

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists affected Cisco platforms. The right column indicates whether a release is affected by the vulnerability that is described in this advisory and the first release that includes the fix for this vulnerability. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco Platform	First Fixed Release
800 Series Industrial ISRs	15.9(3)M11
Catalyst 9100 Family of Access Points (COS-AP)	17.15.2
CGR1000 Compute Modules	15.9(3)M12 (Aug 2025)
IC3000 Industrial Compute Gateways	1.5.2
IOS XE–based devices configured with IOx	17.9.7 17.12.5 17.15.3 17.16.1 For more information, see the Cisco IOS and IOS XE Software Checker in the next section
IR510 WPAN Industrial Routers	Future release

The Cisco Product Security Incident Response Team (PSIRT) validates only the affected and fixed release information that is documented in this advisory.

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 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 by Michael Deviveiros of Cisco during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-dos-95Fqnf7b

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

Resources and Legal

Feedback

Help

Terms & Conditions

Privacy

Cookies / Do not sell or share my personal data

Accessibility

Trademarks

Supply Chain Transparency

Newsroom

Sitemap