Cisco Security Advisory

Cisco IOS Software Industrial Ethernet Switch Device Manager Privilege Escalation Vulnerability

High

Advisory ID:
cisco-sa-ios-http-privesc-wCRd5e3

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwj97907

CVE-2025-20164

CWE-862

CVSS Score:
Base 8.3

Download CSAF Email

Summary

A vulnerability in the Cisco Industrial Ethernet Switch Device Manager (DM) of Cisco IOS Software could allow an authenticated, remote attacker to elevate privileges.

This vulnerability is due to insufficient validation of authorizations for authenticated users. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to elevate privileges to privilege level 15.

To exploit this vulnerability, the attacker must have valid credentials for a user account with privilege level 5 or higher. *Read-only* DM users are assigned privilege level 5.

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-ios-http-privesc-wCRd5e3

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 Industrial Ethernet Series Switches if they are running a vulnerable release of Cisco IOS Software and have HTTP enabled:

- IE 2000 Series
- IE 4000 Series
- IE 4010 Series
- IE 5000 Series

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 HTTP server feature is enabled.

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 running on devices not listed in the Vulnerable Products section of this advisory
- IOS XE Software
- IOS XR Software
- Meraki products
- NX-OS Software

Workarounds

There are no workarounds that address this vulnerability. However, there is a mitigation.

Disabling the HTTP Server feature eliminates the attack vector for this vulnerability 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.

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

Cisco would like to thank Jacek Strzalkowski of Rockwell Automation for reporting this vulnerability.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-privesc-wCRd5e3

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

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