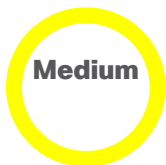




# Cisco IOS XE Software Model-Driven Programmability Authorization Bypass Vulnerability



**Advisory ID:**  
cisco-sa-netconf-nacm-bypass-TGZV9pmQ

**First Published:**  
2025 May 7 16:00 GMT

**Version 1.0:** [Final](#)

**Workarounds:** No workarounds available

**Cisco Bug IDs:**  
[CSCWi33204](#)

CVE-2025-20214

CWE-639

**CVSS Score:**  
[Base 4.3](#) 

[Download CSAF](#)

[Email](#)

## ^ Summary

A vulnerability in the Network Configuration Access Control Module (NACM) of Cisco IOS XE Software could allow an authenticated, remote attacker to obtain unauthorized *read* access to configuration or operational data.

This vulnerability exists because a subtle change in inner API call behavior causes results to be filtered incorrectly. An attacker could exploit this vulnerability by using either NETCONF, RESTCONF, or gRPC Network Management Interface (gNMI) protocols and query data on paths that may have been denied by the NACM configuration. A successful exploit could allow the attacker to access data that should have been restricted according to the NACM configuration.

**Note:** This vulnerability requires that the attacker obtain the credentials from a valid user with privileges lower than 15, and that NACM was configured to provide restricted *read* access for that user.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-netconf-nacm-bypass-TGZV9pmQ>

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 devices if they were running a vulnerable release of Cisco IOS XE Software and had an NACM policy enabled that provides restricted *read* access to lower-privileged users.

For information about which Cisco software releases are vulnerable, see the [Fixed Software](#) section of this advisory.

### 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

## ^ 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-netconf-nacm-bypass-TGZV9pmQ>

### ^ Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-MAY-07

### ^ Legal Disclaimer

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A standalone copy or paraphrase of the text of this document that omits the distribution URL is an uncontrolled copy and may lack important information or contain factual errors. The information in this document is intended for end users of Cisco products.

► 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

