Cisco Security Advisory

Cisco IOS XE Software Bootstrap Arbitrary File Write Vulnerability

Medium

Advisory ID:
cisco-sa-bootstrap-KfgxYgdh

First Published:
2025 May 7 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwj60286

CVE-2025-20155

CWE-1287

CVSS Score:
Base 6.0

Download CSAF

Email

Summary

A vulnerability in the bootstrap loading of Cisco IOS XE Software could allow an authenticated, local attacker to write arbitrary files to an affected system.

This vulnerability is due to insufficient input validation of the bootstrap file that is read by the system software when a device is first deployed in SD-WAN mode or when an administrator configures SD-Routing on the device. An attacker could exploit this vulnerability by modifying a bootstrap file generated by Cisco Catalyst SD-WAN Manager, loading it into the device flash, and then either reloading the device in a green field deployment in SD-WAN mode or configuring the device with SD-Routing. A successful exploit could allow the attacker to perform arbitrary file writes to the underlying operating system.

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-bootstrap-KfgxYgdh

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 supported either Cisco IOS XE Catalyst SD-WAN or SD-Routing functionality, regardless of device configuration.

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 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

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 by Jakub Marciniszyn of Cisco during internal security testing.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootstrap-KfgxYgdh

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