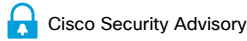


Updated: October 13, 2023 Document ID: 1695833233102185

[Bias-Free Language](#)



Cisco IOS and IOS XE Software Command Authorization Bypass Vulnerability



Advisory ID:
cisco-sa-aaascp-Tyj4fEJm

First Published:
2023 September 27 16:00 GMT

Last Updated:
2023 October 13 13:36 GMT

Version 1.1: Final

Workarounds: Yes

Cisco Bug IDs:
CSCwe55871

CVE-2023-20186

CWE-285

CVSS Score:
Base 8.0 [Click Icon to Copy Verbose Score](#)
CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H/E:X/RL:X/RC:X

[Download CSAF](#)

[Email](#)

Summary

A vulnerability in the Authentication, Authorization, and Accounting (AAA) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to bypass command authorization and copy files to or from the file system of an affected device using the Secure Copy Protocol (SCP).

This vulnerability is due to incorrect processing of SCP commands in AAA command authorization checks. An attacker with valid credentials and level 15 privileges could exploit this vulnerability by using SCP to connect to an affected device from an external machine. A successful exploit could allow the attacker to obtain or change the configuration of the affected device and put files on or retrieve files from the affected device.

Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.

This advisory is available at the following link:

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaascp-Tyj4fEJm>

This advisory is part of the September 2023 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: September 2023 Semiannual Cisco IOS and IOS XE Software Security Advisory Bundled Publication.

Affected Products

Vulnerable Products

This vulnerability affects Cisco products if they are running a vulnerable release of Cisco IOS Software or

Cisco IOS XE Software (in either autonomous mode or controller mode) and have both SCP server functionality and AAA command authorization enabled. However, whether the device is exploitable is dependent on how the TACACS+ profiles for each user are configured. For more information, see the Details section of this advisory.

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

Determine the SCP Server Configuration

To determine whether a device is configured to enable the SCP server, log in to the device and use the **show running-config | include ip scp server enable** command in the CLI. If the device is configured to enable the SCP server, the output will include the **ip scp server enable** command, as shown in the following example:

```
Router# show running-config | include ip scp server enable
ip scp server enable
Router#
```

If the **show running-config | include ip scp server enable** command does not return any output, the device is not configured to enable the SCP server.

Determine the AAA Configuration

To determine whether a device is configured to use AAA for command authorization, log in to the device and use the **show running-config | include aaa authorization commands** command in the CLI. If the command returns any output, the device is configured to use AAA command authorization, as shown in the following example:

```
Router# show running-config | include aaa authorization commands
aaa authorization commands 15 ISE_aaa group ISESERVER local
Router#
```

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 XR Software
- Meraki products
- NX-OS Software

^ Details

When the SCP server is enabled, a user who has appropriate authorization can copy any file to or from the Cisco IOS file system, including images and configurations. Only users who are assigned privilege level 15 are allowed to use the SCP server. Administrators may further restrict what actions an authenticated user may do by enforcing command authorization. Command authorization is enforced by privilege level.

The impact to a customer from this vulnerability is dependent on how their policies for privilege level 15 users are defined. In a scenario where the device has restrictions on privilege level 15 users that prevent them from viewing or changing the configuration, a user could change the configuration by obtaining the configuration through SCP, making changes to the configuration locally, and then copying the configuration back to the device using SCP.

If AAA command authorization is enabled, the SCP command should be processed by the configuration line **aaa authorization commands 15**, given that the SCP user must be a privilege level 15 user. However, due to this vulnerability, the request is handled by the configuration line **aaa authorization commands 0** instead.

SCP client functionality is not affected.

SSH server and client functionality is not affected.

^ Workarounds

There is a workaround and a mitigation that address this vulnerability.

As a workaround for this vulnerability, enable privilege level 0 command authorization checks. To force the AAA server to check SCP server commands, use the configuration command **aaa authorization commands 0** and configure the appropriate command policy to prevent a user from using SCP server commands. To allow or deny file uploads or downloads through SCP, add filters to the AAA configuration for the commands **scp -f** and **scp -t**.

As a mitigation for this vulnerability, disable the SCP server functionality using the configuration command **no ip scp server enable**. Administrators could then use the SCP client functionality on the affected device to copy images or configurations to or from the router.

While this workaround and this mitigation have been deployed and were 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 Hendrik Van Belleghem for reporting this vulnerability.

^ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaascp-Tyj4fEJm>

^ Revision History

Version	Description	Section	Status	Date
1.1	Added attribution.	Source	Final	2023-OCT-13
1.0	Initial public release.	—	Final	2023-SEP-27

^ 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](#)

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](#)



