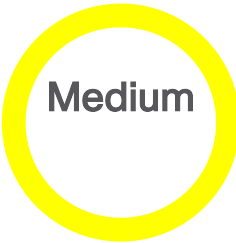




# Cisco Application Policy Infrastructure Controller Vulnerabilities



**Advisory ID:**  
cisco-sa-apic-multi-vulns-9ummtg5

**First Published:**  
2025 February 26 16:00 GMT

**Version 1.0:**    [Final](#)

**Workarounds:**    No workarounds available

**Cisco Bug IDs:**  
[CSCwk18862](#) , [CSCwk18863](#) , [CSCwk18864](#) , [More...](#)

CVE-2025-20116


CVE-2025-20117

CVE-2025-20118

[More...](#)

CWE-77

CWE-79

**CVSS Score:**  
[Base 6.0](#) 

[Download CSAF](#)

[Email](#)

## ^ Summary

Multiple vulnerabilities in Cisco Application Policy Infrastructure Controller (APIC) could allow an authenticated attacker to access sensitive information, execute arbitrary commands, cause a denial of service (DoS) condition, or perform cross-site scripting (XSS) attacks. To exploit these vulnerabilities, the attacker must have valid administrative credentials.

For more information about these vulnerabilities, see the [Details](#) section of this advisory.

Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.

This advisory is available at the following link:  
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-multi-vulns-9ummtg5>

Feedback

## ^ Affected Products

### Vulnerable Products

At the time of publication, these vulnerabilities affected Cisco APIC, regardless of device configuration.

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.

### Products Confirmed Not Vulnerable

Only products listed in the [Vulnerable Products](#) section of this advisory are known to be affected by these vulnerabilities.

## ^ Details

Details about the vulnerabilities are as follows:

### CVE-2025-20119: Cisco APIC Authenticated Local DoS Vulnerability

A vulnerability in the system file permission handling of Cisco APIC could allow an authenticated, local attacker to overwrite critical system files, which could cause a DoS condition. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to a race condition with handling system files. An attacker could exploit this vulnerability by doing specific operations on the file system. A successful exploit could allow the attacker to overwrite system files, which could lead to the device being in an inconsistent state and cause a DoS condition.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): [CSCwk18865](#)  
CVE ID: CVE-2025-20119  
SIR: Medium  
CVSS Base Score: 6.0  
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

CVE-2025-20117: Cisco APIC Authenticated Command Injection Vulnerability

A vulnerability in the CLI of Cisco APIC could allow an authenticated, local attacker to execute arbitrary commands as *root* on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of *root*.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): [CSCwk18862](#)  
CVE ID: CVE-2025-20117  
Security Impact Rating (SIR): Medium  
CVSS Base Score: 5.1  
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:N

CVE-2025-20116: Cisco APIC Stored XSS Vulnerability

A vulnerability in the web UI of Cisco APIC could allow an authenticated, remote attacker to perform a stored XSS attack on an affected system. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to improper input validation in the web UI. An authenticated attacker could exploit this vulnerability by injecting malicious code into specific pages of the web UI. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web UI or access sensitive, browser-based information.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): [CSCwk18863](#)  
CVE ID: CVE-2025-20116  
SIR: Medium  
CVSS Base Score: 4.8  
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

CVE-2025-20118: Cisco APIC Authenticated Information Disclosure Vulnerability

A vulnerability in the implementation of the internal system processes of Cisco APIC could allow an authenticated, local attacker to access sensitive information on an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials.

This vulnerability is due to insufficient masking of sensitive information that is displayed through system CLI commands. An attacker could exploit this vulnerability by using reconnaissance techniques at the device CLI. A successful exploit could allow the attacker to access sensitive information on an affected device that could be used for additional attacks.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Bug ID(s): [CSCwk18864](#)  
CVE ID: CVE-2025-20118  
SIR: Medium  
CVSS Base Score: 4.4  
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

^ Workarounds

There are no workarounds that address these vulnerabilities.

^ 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

In the following tables, the left column lists Cisco software releases. 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 APIC Releases	First Fixed Release
5.3 and earlier	Migrate to a fixed release.
6.0	6.0(8e)
6.1	6.1(2f)

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

^ Exploitation and Public Announcements

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that is described in this advisory.

^ Source

Cisco would like to thank Jean-Michel Huguet and Jorge Escabias from NATO Cyber Security Centre (NCSC) for reporting these vulnerabilities.

^ URL

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-multi-vulns-9ummtg5>

^ Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2025-FEB-26

Feedback

^ 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

