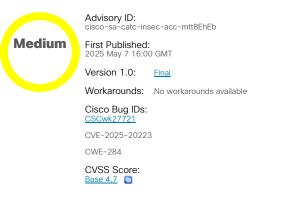


Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco Catalyst Center Insufficient Access Control Vulnerability



Download CSAF

Email

Summary

A vulnerability in Cisco Catalyst Center, formerly Cisco DNA Center, could allow an authenticated, remote attacker to read and modify data in a repository that belongs to an internal service of an affected device.

This vulnerability is due to insufficient enforcement of access control on HTTP requests. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.

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-catc-insec-acc-mtt8EhEb

Affected Products

Vulnerable Products

At the time of publication, this vulnerability affected Cisco Catalyst Center deployments that have Disaster Recovery enabled. Disaster Recovery is not enabled by default.

For information about which Cisco software releases were vulnerable at the time of publication, see the <u>Fixed Software</u> 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.

Determine Whether Disaster Recovery Is Enabled

To determine whether Disaster Recovery is enabled, choose System > Disaster Recovery in the Cisco Catalyst Center GUI and check the status of the configuration. Disaster Recovery is not configured and the device is not affected if one of the following is true:

- The Disaster Recovery option is absent.
- The status of Disaster Recovery is Unconfigured, and all the sites in the topology have the status Unregistered.

Any other status indicates that the device is affected by this vulnerability.

Products Confirmed Not Vulnerable

Only products listed in the <u>Vulnerable Products</u> section of this advisory are known to be affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

∧ Fixed Software

When <u>considering software upgrades</u>, customers are advised to regularly consult the advisories for Cisco products, which are available from the <u>Cisco Security Advisories page</u>, 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

At the time of publication, the release information in the following table was accurate. See the Details section in the bug ID(s) at the top of this advisory for the most complete and current information.

The left column lists Cisco software releases, and the right column indicates whether a release was affected by the vulnerability that is described in this advisory and which release included the fix for this vulnerability.

Cisco Catalyst Center Release	First Fixed Release
Earlier than 2.3.7.7	2.3.7.7

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 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-catc-insecacc-mtt8EhEb

∧ 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 4 star

0

3 star	0
2 star	0
1 star	
i 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					
	Ø	\mathbb{X}	in	D	0

©2025 Cisco Systems, Inc.