Cisco Security Advisory

Cisco Webex Services Certificate Validation Vulnerability

Critical

Advisory ID:
cisco-sa-webex-cui-cert-8jSZYhWL

First Published:
2026 April 15 16:00 GMT

Last Updated:
2026 April 16 18:52 GMT

Version 1.1: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwt37111

CVE-2026-20184

CWE-295

CVSS Score:
Base 9.8

Download CSAF

Email

Summary

A vulnerability in the integration of single sign-on (SSO) with Control Hub in Cisco Webex Services could have allowed an unauthenticated, remote attacker to impersonate any user within the service.

This vulnerability existed because of improper certificate validation. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by connecting to a service endpoint and supplying a crafted token. A successful exploit could have allowed the attacker to gain unauthorized access to legitimate Cisco Webex services.

Cisco has addressed this vulnerability in the Cisco Webex service. However, customer action is necessary for affected organizations that are using trust anchors with their SSO integration.

There are no workarounds that address this vulnerability.

To avoid service interruption, customers who are using trust anchors with their SSO integration should upload a new identity provider (IdP) SAML certificate to Control Hub. For more information, see Manage single sign-on integration in Control Hub.

This advisory is available at the following link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL

Affected Products

Vulnerable Products

This vulnerability affected Cisco Webex Services, which are cloud-based, when they were configured to use trust anchors within the SSO integration with Control Hub.

Determine Whether Trust Anchors Are in Use

Only customers who use trust anchors were affected by this vulnerability. To determine whether trust anchors are in use, log in to the Webex Control Hub and verify the SSO configuration.

Products Confirmed Not Vulnerable

Only products listed in the Vulnerable Products section of this advisory are known to have been affected by this vulnerability.

Workarounds

There are no workarounds that address this vulnerability.

Fixed Software

Cisco has addressed this vulnerability in Cisco Webex Services, which are cloud

To avoid service interruption, customers who are using trust anchors with their SSO integration should upload a new identity provider (IdP) SAML certificate to Control Hub. For more information, see Manage single sign-on integration in Control Hub.

Customers who need additional information are advised to contact the Cisco Technical Assistance Center (TAC) or their contracted maintenance providers.

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-webex-cui-cert-8jSZYhWL

Revision History

Version	Description	Section	Status	Date
1.1	Added information about trust anchor usage.	Summary, Vulnerable Products, Fixed Software	Final	2026-APR-16
1.0	Initial public release.	-	Final	2026-APR-15

Legal Disclaimer

SOFTWARE DOWNLOADS AND TECHNICAL SUPPORT

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. Please note that customers may download only software that was procured from Cisco directly or through a Cisco authorized reseller or partner and for which the license is still valid.

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 Technical Assistance Center (TAC). 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.

When considering software upgrades, customers are advised to regularly consult the advisories for the relevant Cisco products 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.

LEGAL DISCLAIMER DETAILS

CISCO DOES NOT MAKE ANY EXPRESS OR IMPLIED GUARANTEES OR WARRANTIES OF ANY KIND, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, CISCO DOES NOT GUARANTEE THE ACCURACY OR COMPLETENESS OF THIS INFORMATION. THIS DOCUMENT IS PROVIDED ON AN " AS IS" BASIS. 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.

Copies or summaries of the information contained in this Security Advisory may lack important information or contain factual errors. Customers are advised to visit the Cisco Security Advisories page for the most recent version of this Security Advisory. The Cisco Product Security Incident Response Team (PSIRT) assesses only the affected and fixed release information that is documented in this advisory. See the Cisco Security Vulnerability Policy for more information.