Cisco Security Advisory

Cisco Unity Connection Remote Code Execution and Server-Side Request Forgery Vulnerabilities

Advisory ID:
cisco-sa-unity-rce-ssrf-hENhuASy

First Published:
2026 May 6 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwq36774 , CSCwq36834

CVE-2026-20034

CVE-2026-20035

CWE-35

CWE-918

CVSS Score:
Base 8.8

Download CSAF

Email

Summary

Multiple vulnerabilities in Cisco Unity Connection could allow a remote attacker to execute arbitrary code on or conduct server-side request forgery (SSRF) attacks through an affected device.

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-unity-rce-ssrf-hENhuASy

Affected Products

Vulnerable Products

CVE-2026-20034: This vulnerability affects Cisco Unity Connection, regardless of device configuration.

CVE-2026-20035: This vulnerability affects Cisco Unity Connection if Web Inbox is enabled. Web Inbox is enabled by default.

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

Determine Whether Web Inbox Is Enabled

To determine whether Web Inbox is enabled, complete the following steps:

1. Connect to the Cisco Unity Connection Administration interface and choose **Class of Service**.
2. Choose the predefined class of service **Voice Mail User COS** or a custom class of service.
3. In the **Licensed Features** section, scroll down to **Allow Users to Use the Web Inbox and RSS Feeds**.

If the **Allow Users to Use the Web Inbox and RSS Feeds** box is checked, the feature is enabled.

Products Confirmed Not Vulnerable

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

Details

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit the other vulnerability. In addition, a software release that is affected by one of the vulnerabilities may not be affected by the other vulnerability.

Details about the vulnerabilities are as follows:

CVE-2026-20034: Cisco Unity Connection Remote Code Execution Vulnerability

A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to execute arbitrary code on an affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to execute arbitrary code as *root*, possibly resulting in the complete compromise of a targeted device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.

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

Bug ID(s): CSCwq36774
CVE ID: CVE-2026-20034
Security Impact Rating (SIR): High
CVSS Base Score: 8.8
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2026-20035: Cisco Unity Connection SSRF Vulnerability

A vulnerability in the web UI of Cisco Unity Connection Web Inbox could allow an unauthenticated, remote attacker to conduct SSRF attacks through an affected device.

This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to send arbitrary network requests that are sourced from the affected device.

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

Bug ID(s): CSCwq36834
CVE ID: CVE-2026-20035
Security Impact Rating (SIR): High
CVSS Base Score: 7.2
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N

Workarounds

There are no workarounds that address these vulnerabilities.

Fixed Software

Cisco considers any workarounds and mitigations (if applicable) to be temporary solutions until an upgrade to a fixed software release is available. To fully remediate these vulnerabilities and avoid future exposure as described in this advisory, Cisco strongly recommends that customers upgrade to the fixed software indicated in this advisory.

Fixed Releases

In the following table, the left column lists Cisco software releases. The right column indicates whether a release is affected by the vulnerabilities that are described in this advisory and the first release that includes the fix for these vulnerabilities. Customers are advised to upgrade to an appropriate fixed software release as indicated in this section.

Cisco Unity Connection Release	First Fixed Release
12.5 and earlier	Migrate to a fixed release.
14.0	14SU5
15.0	15SU4 or apply patch file:[1] ciscocm.cuc.V15_CSCwq36774-CSCwq36834_C0277-1.zip

1. Patches are version-specific. Consult the README attached to the patch for details.

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 are described in this advisory.

Source

Cisco would like to thank security researcher Jahmel Harris of NATO Cyber Security Centre (NCSC) for reporting these vulnerabilities.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-unity-rce-ssrf-hENhuASy

Revision History

Version	Description	Section	Status	Date
1.0	Initial public release.	-	Final	2026-MAY-06

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.

- ▶ Cisco Security Vulnerability Policy
- ▶ Subscribe to Cisco Security Notifications
- ▶ Related to This Advisory