Cisco Security Advisory

Cisco Unity Connection Cross-Site Scripting, Open Redirect, and SQL Injection Vulnerabilities

Medium

Advisory ID:
cisco-sa-unity-vulns-n2EJSbbw

First Published:
2026 April 15 16:00 GMT

Version 1.0: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwq36796 , CSCwq36822 , CSCwq36828

CVE-2026-20059

CVE-2026-20060

CVE-2026-20061

CWE-601

CWE-79

CWE-89

CVSS Score:
Base 6.1

Download CSAF

Email

Summary

Multiple vulnerabilities in Cisco Unity Connection could allow a remote attacker to conduct a cross-site scripting (XSS) attack, an open redirect attack, and an SQL injection attack.

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-vulns-n2EJSbbw

Affected Products

Vulnerable Products

At the time of publication, these vulnerabilities affected Cisco Unity Connection, 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

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

Details about the vulnerabilities are as follows:

CVE-2026-20059: Cisco Unity Connection Reflected XXS Vulnerability

A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a user of the interface.

This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute script code in the context of the affected interface or access sensitive, browser-based

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

Bug ID: CSCwq36822
CVE ID: CVE-2026-20059
Security Impact Rating (SIR): Medium
CVSS Base Score: 6.1
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2026-20060: Cisco Unity Connection Open Redirect Vulnerability

A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to redirect a user to a malicious web page.

This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious web page.

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

Bug ID: CSCwq36828
CVE ID: CVE-2026-20060
Security Impact Rating (SIR): Medium
CVSS Base Score: 4.7
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N

CVE-2026-20061: Cisco Unity Connection SQL Injection Vulnerability

A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to perform an SQL injection attack against an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device.

This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP(S) request to the web-based management interface of an affected device. A successful exploit could allow the attacker to view data on the affected device.

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

Bug ID: CSCwq36796
CVE ID: CVE-2026-20061
Security Impact Rating (SIR): Medium
CVSS Base Score: 4.3
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/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

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.

In the following table, the left column lists Cisco software releases. The center and right columns indicate 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.

Cisco Unity Connection Release	First Fixed Release for CVE-2026-20059 and CVE-2026-20061	First Fixed Release for CVE-2026-20060
12.5	Migrate to a fixed release.	Migrate to a fixed release.
14	14SU6	14SU5
15	15SU4	15SU4

The Cisco Product Security Incident Response Team (PSIRT) validates only the a ted 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

Cisco would like to thank 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-vulns-n2EJSbbw

Revision History

Version	Description	Section	Status	Date
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.

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