Cisco Security Advisory

Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerabilities

Medium

Advisory ID:
cisco-sa-ise-xss-42tgsdMG

First Published:
2025 February 5 16:00 GMT

Last Updated:
2026 May 5 18:21 GMT

Version 1.1: Final

Workarounds: No workarounds available

Cisco Bug IDs:
CSCwm38652

CVE-2025-20204

CVE-2025-20205

CWE-79

CVSS Score:
Base 4.8

Download CSAF

Email

Summary

Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface.

These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit these vulnerabilities by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid administrative credentials.

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-ise-xss-42tgsdMG

Affected Products

Vulnerable Products

At the time of publication, these vulnerabilities affected Cisco ISE, 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.

Cisco has confirmed that these vulnerabilities do not affect Cisco ISE Passive Identity Connector.

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

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 center and right columns indicate whether a release was affected by one of the vulnerabilities that are described in this advisory and which release included the fix for that vulnerability.

Cisco ISE Software Release	First Fixed Release
3.4 and earlier	Migrate to a fixed release.
3.5	Not vulnerable.

For instructions on upgrading a device, see the Upgrade Guides on the Cisco Identity Service Engine support page.

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

CVE-2025-20204: Cisco would like to thank Laura Rowieska of ING Hubs Poland for reporting this vulnerability. Cisco would also like to thank Dan Marin, Teodor Cervinski, George Jubleanu, and Cristian Mocanu of Deloitte for independently reporting this vulnerability.

CVE-2025-20205: Cisco would like to thank Laura Rowieska of ING Hubs Poland for reporting this vulnerability.

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-42tgsdMG

Revision History

Version	Description	Section	Status	Date
1.1	Updated bug ID and fixed release tables.	Heading and Fixed Releases	Final	2026-MAY-05
1.0	Initial public release.	-	Final	2025-FEB-05

Legal Disclaimer

▶ Cisco Security Vulnerability Policy

▶ Subscribe to Cisco Security Notifications

▶ Related to This Advisory

Quick Links