



# Cisco Identity Services Engine Stored Cross-Site Scripting Vulnerability

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2025-20204
<b>State</b>	PUBLISHED
<b>Assigner</b>	cisco
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-02-05 17:15:26 UTC
<b>Updated</b>	2026-05-06 19:16:35 UTC

**Description** Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an auth

## Risk And Classification

**Primary CVSS:** v3.1 4.8 MEDIUM from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

**Problem Types:** CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	psirt@cisco.com	Secondary	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSSV3_1	4.8	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

High

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Identity Services Engine	All	All	All	All
Application	Cisco	Identity Services Engine	3.2.0	-	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch1	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch2	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch3	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch4	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch5	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch6	All	All
Application	Cisco	Identity Services Engine	3.2.0	patch7	All	All
Application	Cisco	Identity Services Engine	3.3.0	-	All	All
Application	Cisco	Identity Services Engine	3.3.0	patch1	All	All
Application	Cisco	Identity Services Engine	3.3.0	patch2	All	All
Application	Cisco	Identity Services Engine	3.4.0	-	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p1	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p2	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p3	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p4	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0 p1	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p5	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0 p3	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0 p2	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0 p6	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.0.0	Not specified



CNA	Cisco	Cisco Identity Services Engine Software	affected 3.3 Patch 11	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.4 Patch 6	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.2 Patch 10	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0 p72	Not specified
CNA	Cisco	Cisco Identity Services Engine Software	affected 3.1.0 p11	Not specified

## References

Reference	Source	Link	Tag
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xs...	psirt@cisco.com	sec.cloudapps.cisco.com	Ver
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

## Additional Advisory Data

### Exploits

**CNA:** The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in this advisory.

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)