Cisco ISE Stored XSS Flaw Could Let Attackers Target Admin Sessions

TL;DR

Cisco ISE contains a medium-severity stored cross-site scripting vulnerability (CVE-2025-20267) that could let an attacker with admin credentials inject malicious scripts into the web management interface.

There are no workarounds, patches are available.

Overview

Cisco has confirmed a stored cross-site scripting (XSS) vulnerability (CVE-2025-20267, CVSS 4.8) within the web management interface of Identity Services Engine (ISE). This issue stems from inadequate validation of user input, making it possible for an authenticated attacker to insert malicious scripts into certain interface pages. If successful, this could let the attacker execute code in a user's browser session or access sensitive browser-based data. The attacker must have valid administrative credentials to exploit this flaw.

Affected Products

- Cisco Identity Services Engine (ISE) 3.1 and earlier
- Cisco Identity Services Engine (ISE) 3.2
- Cisco Identity Services Engine (ISE) 3.3
- Cisco Identity Services Engine (ISE) 3.4

This isn't a vulnerability that is critical or being exploited, but that doesn't mean you should ignore it. XSS flaws like CVE-2025-20267 can still lead to stolen session tokens or browser-based attacks if an admin account gets compromised. It's important for organizations to check who really needs admin access, cut down that list, and update your passwords. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** - Apply Cisco's software updates. Find patch guidance in Cisco's advisory.
- Review and restrict admin access where possible.
- Monitor for suspicious activity tied to admin accounts.

- Educate users on XSS risks and safe browser practices when interacting with admin interfaces.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] - The attacker may have leveraged valid credentials to gain admin access to Cisco ISE.

Execution

- User Execution [T1204] - The attacker may have relied on a legitimate user interacting with a compromised page to trigger malicious script execution.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability could affect any organization using Cisco ISE, including

- Education
- Healthcare
- Retail and eCommerce
- Government
- Finance
- Manufacturing
- Energy
- Legal and Professional Services

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security

professionals to identify and respond to threats across a broader attack surface.
    - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
    - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
    - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Identity Services Stored Cross-Site Scripting Vulnerability

NVD - CVE-2025-20267