Cisco ISE Flaws Let Attackers Execute Code and Access Sensitive Files with Admin Access

TL;DR

There are two vulnerabilities in Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (CVE-2026-20147, CVSS 9.9 and CVE-2026-20148, CVSS 4.9) that allow an authenticated attacker to execute commands or read sensitive files on affected systems.

Both issues require valid administrative credentials, but the impact is severe once access is obtained.

Overview

There are vulnerabilities in Cisco Identity Services Engine (ISE) and ISE Passive Identity Connector (CVE-2026-20147, CVSS 9.9 and CVE-2026-20148, CVSS 4.9) that could allow an authenticated attacker to execute arbitrary commands or read sensitive files on affected systems.

Affected Products

- Cisco Identity Services Engine (ISE) versions prior to:
  - 3.1 Patch 11
  - 3.2 Patch 10
  - 3.3 Patch 11
  - 3.4 Patch 6
  - 3.5 Patch 3
- Cisco ISE Passive Identity Connector (ISE-PIC) (same version ranges apply)

CVE-2026-20147 is a remote code execution vulnerability caused by insufficient validation of user input. An attacker with administrative credentials can send a crafted HTTP request to execute commands on the underlying operating system. This can lead to user-level access and potential escalation to root. In single-node deployments, exploitation may also cause the system to become unavailable, preventing new endpoints from authenticating to the network.

CVE-2026-20148 is a path traversal vulnerability caused by improper input validation. An attacker with administrative access can use crafted requests to read arbitrary files from the system, which may expose sensitive configuration data or credentials.

These vulnerabilities are not linked and can be exploited separately. While administrative access is required, this type of access is often targeted by threat actors during post-compromise activity. Aspire recommends patching immediately.

Aspire Protects

- Apply Cisco security updates immediately to the fixed versions listed above. See Cisco's advisory for patch guidance.
- Audit administrative accounts for unauthorized or suspicious access.
- Rotate administrative credentials, especially if compromise is suspected.
- Monitor ISE systems for unusual HTTP requests or command execution activity.
- Review logs for unauthorized file access attempts.
- Restrict administrative access to trusted networks and enforce MFA.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may use compromised administrative credentials to access the ISE system

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute system-level commands through crafted HTTP requests

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – The attacker may escalate privileges from user-level access to root

Collection

- Data from Local System [T1005] – The attacker may read sensitive files from the system using path traversal techniques

IoCs

There are no known IoCs 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

Organizations that rely on centralized network authentication and access control are most at risk, including:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Government
- Retail

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 Engine Remote Code Execution and Path Traversal Vulnerabilities]