Cisco Identity Services Engine (ISE) Vulnerabilities

Overview

Cisco just patched two serious vulnerabilities in its Identity Services Engine (ISE) that could let attackers with basic admin credentials execute commands, change configurations, and even reboot devices.

CVE-2025-20124 (CVSS 9.9)

- Impact – Allows an authenticated attacker with read-only administrative credentials to execute arbitrary commands as the root user.
- Cause – Insecure deserialization of user-supplied Java byte streams in an API. Attackers can send a crafted serialized Java object to an affected API to achieve command execution and privilege escalation.

CVE-2025-20125 (CVSS 9.1)

- Impact – Attackers with valid read-only credentials can access sensitive information, modify system configurations, and force device reboots.
- Cause – Lack of authorization checks in a specific API and improper input validation. The vulnerability is exploited via crafted HTTP requests to a vulnerable API endpoint.

Affected Products

- Vulnerable - Cisco ISE and ISE-PIC (all configurations)
- Not Vulnerable - Cisco ISE 3.4 and later

If an organization fails to patch these vulnerabilities, attackers with basic admin credentials could execute commands as root, gaining complete control over the system. Since no workarounds exist, leaving this unpatched is essentially leaving the door wide open for an attacker.

Aspire Protects

- **Patch –** Upgrade to a fixed Cisco ISE version as listed in Cisco's advisory.
- Limit access to Cisco ISE administrative interfaces to trusted networks.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may use stolen or weak credentials to gain access to Cisco ISE with read-only administrative privileges.

Persistence

- Create or Modify System Process [T1543] – The attacker could modify Cisco ISE configurations to maintain persistent access.

Impact

- Service Stop [T1489] – Exploiting CVE-2025-20125 could allow an attacker to restart Cisco ISE nodes, disrupting authentication services.
- Data Destruction [T1485] – Attackers with root access could delete logs or tamper with authentication databases.

IoCs

There are no known IoCs associated with the above vulnerabilities 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

- Communications
- Government
- Energy
- Manufacturing
- Transportation
- Utilities
- Finance
- Healthcare
- And others

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 Insecure Java Deserialization and Authorization Bypass Vulnerabilities

NVD - CVE-2025-20124