Critical Cisco Identity Services Engine Critical RCE Vulnerabilities

Overview

This week, Cisco publicized two critical vulnerabilities (CVE-2025-20281 and CVE-2025-20282) impacting Cisco ISE and ISE-PIC. Both vulnerabilities have received a **maximum CVSS score of 10.0**, due to their severity and ease of exploitation. Successful exploitation provides attackers with root-level access to vulnerable systems, significantly compromising security and allowing attackers to have extensive unauthorized control.

TL;DR

Cisco released patches for two critical vulnerabilities (CVE-2025-20281, CVE-2025-20282) in Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC), allowing unauthenticated attackers to execute code as root.

Immediate patching is recommended, as no workarounds are available.

Vulnerability Breakdown

- CVE-2025-20281 (CVSS 10.0) – This vulnerability stems from improper validation of input in a publicly exposed API. An attacker could exploit this flaw remotely without credentials by sending maliciously crafted requests, leading directly to arbitrary code execution as root. Cisco ISE and ISE-PIC versions 3.3 and later are affected.

- CVE-2025-20282 (CVSS 10.0) – This vulnerability results from inadequate checks within an internal API that fails to validate uploaded files properly. The flaw lets attackers place and execute malicious files in privileged system directories. It specifically affects Cisco ISE and ISE-PIC version 3.4.

The severity and simplicity of exploitation for these vulnerabilities mean organizations using Cisco ISE need to patch **immediately**. Patching will avoid potential system compromise, unauthorized control, and significant damage to security operations.

Aspire Protects

- **Patch**
  - For CVE-2025-20281 - Update to version 3.3 Patch 6 or version 3.4 Patch 2.
  - For CVE-2025-20282 - Update to version 3.4 Patch 2.
  - Find patch guidance for both vulnerabilities in Cisco's advisory.
- Temporarily limit external access to Cisco ISE APIs where possible, allowing connections only from trusted IP addresses or VPNs until patches are applied.
- Quickly inventory Cisco ISE and ISE-PIC deployments to ensure no vulnerable instances are overlooked during patching.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit vulnerable Cisco ISE APIs remotely without authentication.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute arbitrary code or commands on compromised Cisco ISE systems.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – The attacker may gain immediate root-level access after exploiting these vulnerabilities.

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

Organizations in the following industries commonly using Cisco ISE and ISE-PIC are particularly vulnerable and should apply patches:

- Education
- Healthcare

- Retail and eCommerce
- Government
- Finance
- Manufacturing
- Technology

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 Unauthenticated Remote Code Execution Vulnerabilities

NVD - CVE-2025-20282

NVD - CVE-2025-20281