Cisco Identity Services Engine Static Credential Vulnerability

TL;DR

Cisco ISE deployments in AWS, Azure, and OCI cloud environments were found sharing static admin credentials across instances.The vulnerability is being tracked as CVE-2025-20286.

An unauthenticated attacker could use these credentials to access other cloud ISE environments, change configurations, or disrupt services. A hotfix is available and should be applied immediately.

Overview

A critical vulnerability (CVE-2025-20286, CVSS 9.9) in Cisco Identity Services Engine (ISE) cloud deployments allows attackers to extract static credentials from one instance and use them to access others deployed on the same cloud platform and software version. Cisco has released a hotfix, but no workaround exists beyond patching or reconfiguring access controls.

Affected Products

- Cisco ISE 3.1, 3.2, 3.3, and 3.4 on AWS
- Cisco ISE 3.2, 3.3, and 3.4 on Azure
- Cisco ISE 3.2, 3.3, and 3.4 on OCI

This flaw stems from how Cisco ISE generates and assigns credentials in cloud deployments. Identical credentials are used across all cloud-based ISE instances running the same version on the same platform. If the Primary Administration node is cloud-hosted, it's vulnerable. On-prem deployments are not affected. Exploitation could lead to configuration tampering and limited admin actions, without authentication.

Cisco has confirmed that proof-of-concept (POC) exploit code is publicly available. No active exploitation has been observed yet, but that window may close quickly. Organizations with ISE cloud deployments could face unauthorized changes to network access policies or data exposure, especially if they haven't applied the patch or isolated access via IP controls. Aspire recommends patching immediately.

Aspire Protects

- **Patch –** Apply the official hotfix for affected versions (Cisco ISE Releases 3.1–3.4).
- If unable to patch immediately, restrict access using cloud security groups and IP allowlists in the ISE interface.
- Do not restore old backups after patching unless new credentials have been saved post-fix.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The attacker may have used shared static credentials from one cloud ISE deployment to gain access to another environment.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may have executed limited administrative commands after gaining access to the ISE system.

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 is most relevant to organizations running Cisco ISE in cloud environments, particularly those in sectors that rely on strict network access controls.

- Financial
- Healthcare
- Education
- Government
- Large Enterprise Networks

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 on Cloud Platforms Static Credential Vulnerability

NVD - CVE-2025-20286