An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2506060163

NCSC Advisory

Vulnerability in Cisco Identity Services Engine

CVE-2025-20286

6th, June 2025

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2025-20286

Published: 2025-06-04

Vendor: Cisco

Product: Identity Services Engine Software

CVSS Score[1]**:** 9.9

Products Affected

Platform	Version
AWS	Cisco ISE version 3.1, 3.2, 3.3 and 3.4
Azure	Cisco ISE version 3.2, 3.3 and 3.4
OCI	Cisco ISE version 3.2, 3.3 and 3.4

Impact

A vulnerability in Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI) cloud deployments of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to access sensitive data, execute limited administrative operations, modify system configurations, or disrupt services within the impacted systems.

This vulnerability exists because credentials are improperly generated when Cisco ISE is being deployed on cloud platforms, resulting in different Cisco ISE deployments sharing the same credentials.

These credentials are shared across multiple Cisco ISE deployments as long as the software release and cloud platform are the same.

An attacker could exploit this vulnerability by extracting the user credentials from Cisco ISE that is deployed in the cloud and then using them to access Cisco ISE that is deployed in other cloud environments through unsecured ports.

A successful exploit could allow the attacker to access sensitive data, execute limited administrative operations, modify system configurations, or disrupt services within the impacted systems.

[1] https://www.first.org/cvss/

Note: If the Primary Administration node is deployed in the cloud, then Cisco ISE is affected by this vulnerability. If the Primary Administration node is on-premises, then it is not affected.

Cisco has released software updates that address this vulnerability. **There are no workarounds that address this vulnerability.**

Common Weakness Enumeration (CWE)[2]: CWE-259: Use of Hard-coded Password

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

- https://nvd.nist.gov/vuln/detail/CVE-2025-20286
- https://www.cve.org/CVERecord?id=CVE-2025-20286
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog