# CVE-2025-20286: Critical Cisco ISE Auth Bypass Flaw Impacts Cloud Deployments on AWS, Azure, and OCI

## Vairav CVE Report

**Date: June 5, 2025**

**Vairav Cyber Threat Intelligence Team**


## Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

## EXECUTIVE SUMMARY

A critical vulnerability, **CVE-2025-20286**, has been identified in Cisco Identity Services Engine (ISE) deployments across major cloud platforms, including Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI). This flaw arises from the use of static credentials in cloud-based deployments, potentially allowing unauthenticated, remote attackers to gain unauthorized access. With a **CVSS score of 9.9**, the exploitation of this vulnerability could lead to unauthorized access to sensitive data, execution of limited administrative operations, modification of system configurations, or disruption of services within the impacted systems.

## VULNERABILITY DETAILS

### CVE-2025-20286

- **Description:** This vulnerability exists due to improperly generated static credentials in Cisco ISE cloud deployments. Specifically, when Cisco ISE is deployed on cloud platforms, the credentials are not uniquely generated per instance. Instead, all instances of a particular release on a specific cloud platform share the same credentials.
- **Impact:** An attacker exploiting this vulnerability could gain unauthorized access to Cisco ISE instances, leading to potential exposure of sensitive data, execution of limited administrative operations, modification of system configurations, or disruption of services.
- **CVSS Score:** 9.9 (Critical)

## AFFECTED VERSIONS

Cisco ISE deployments on cloud platforms are affected as follows:

- **AWS**: Versions 3.1, 3.2, 3.3, and 3.4
- **Microsoft Azure**: Versions 3.2, 3.3, and 3.4
- **Oracle Cloud Infrastructure (OCI)**: Versions 3.2, 3.3, and 3.4

It's important to note that only deployments where the Primary Administration Node is hosted in the cloud are affected. On-premises deployments are not impacted by this vulnerability.

## EXPLOIT DETAILS

The vulnerability stems from the use of static credentials in cloud-based Cisco ISE deployments. Since these credentials are identical across all instances of a specific release on a given cloud platform, an attacker who obtains the credentials from one instance can potentially access other instances. This access could be achieved through unsecured ports or other vulnerabilities, leading to unauthorized access to sensitive data and administrative functionalities.

## RECOMMENDED ACTIONS

**Patch & Upgrade**: Cisco has released security patches addressing this vulnerability. Users are strongly advised to upgrade to the latest versions of Cisco ISE that contain the necessary fixes.

## ADDITIONAL SECURITY MEASURES

- **Restrict Access**: Limit network access to Cisco ISE instances by implementing strict firewall rules and ACLs so only authorized administrators can access the system.
- **Credential Management**: Regularly rotate credentials and avoid using default or static credentials. Implement multi-factor authentication (MFA) where possible.
- **Monitoring and Logging**: Enable detailed logging and monitor for any unauthorized access attempts or unusual activities within the Cisco ISE environment.
- **Configuration Review**: Regularly review and audit system configurations to ensure compliance with security best practices.

## REFERENCES

- https://app.opencve.io/cve/CVE-2025-20286
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

## CONTACT US

**Vairav Technology Security Pvt. Ltd.**

**Cyber Defender from the land of Gurkha**

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com