CYBER ADVISORY

CALIFORNIA CYBERSECURITY INTEGRATION CENTER

Cal OES
GOVERNOR'S OFFICE
OF EMERGENCY SERVICES

*CYBER ADVISORY*

TLP:CLEAR
06 June 2025

## Cisco ISE Cloud Platforms Static Credential Vulnerability

Critical Vulnerability | AWS | Hard-coded Password | Microsoft Azure

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability, CVE-2025-20286 with a CVSS 3.x score of 9.9. The vulnerability affects Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI) cloud deployments of Cisco Identity Services Engine (ISE). CVE-2025-20286 is a use of hard-coded password vulnerability, that improperly generates credentials when Cisco ISE is deployed on cloud platforms, resulting in different Cisco ISE deployments sharing the same credentials.[1] Successful exploitation of this vulnerability could allow an unauthenticated remote user to access sensitive data, execute administrative operations, modify system configuration, or disrupt services within the vulnerable system.[2] Cisco is aware of a proof-of-concept for this vulnerability, however, no active exploitation has been found.[3]

The Cal-CSIC recommends immediately updating to the latest version of Cisco ISE.

For more information on applying security updates please refer to Cisco's Security Advisory.

**Table1: Vulnerable Products**

| Platform | Cisco ISE Releases |
|---|---|
| Amazon Web Services | 3.1, 3.2, 3.3, and 3.4 |
| Microsoft Azure | 3.2, 3.3, and 3.4 |
| Oracle Cloud Infrastructure | 3.2, 3.3, and 3.4 |

## Organization, Source, Reference, and Dissemination Information

| | |
|---|---|
| **Organization Description** | California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state. |
| **Customer Feedback** | If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. |
| **Source Summary Statement** | This report was compiled from a variety of sources, predominately open-source reporting. |
| **Handling Caveats** | **Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |

[1] National Vulnerability Database; "CVE-2025-20286 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2025-20286; accessed 05 June 2025.
[2] The Hacker News; "Critical Cisco ISE Auth Bypass Flaw Impacts Cloud Deployments on AWS, Azure, and OCI"; https://thehackernews.com/2025/06/critical-cisco-ise-auth-bypass-flaw.html; accessed 05 June 2025.
[3] Cisco; "Cisco Identity Services Engine on Cloud Platforms Static Credential Vulnerability"; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7; accessed 05 June 2025.