NATIONAL CSIRT-CY

CVE-2025-20286 **09/06/2025**

Critical Cisco vulnerability in ISE (Identity Services Engine)

Executive Summary

New security updates have been released by Cisco to address a critical vulnerability in ISE. This Vulnerability has been assigned a CVSS score of 9.9/10.

A remote attacker exploiting this vulnerability can gain access to sensitive data, modify configurations or disrupt services. Specifically in Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI) cloud deployments of Cisco Identity Services Engine

As per Cisco, 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.

Affected Products:

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

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-20286

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/259.html

Solutions

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

Please distribute this information among your subsidiaries and partners and also share with us any pertinent information and findings you may have (e.g. IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.