مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Cisco ISE Cloud Deployments

Tracking #:432317358

Date:10-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability (CVE-2025-20286) has been identified in cloud-based deployments of Cisco Identity Services Engine (ISE) across AWS, Microsoft Azure, and Oracle Cloud Infrastructure (OCI).

TECHNICAL DETAILS:

A critical vulnerability (CVE-2025-20286) has been identified in cloud-based deployments of Cisco Identity Services Engine (ISE) across AWS, Microsoft Azure, and Oracle Cloud Infrastructure (OCI). Due to improperly generated static credentials, multiple Cisco ISE deployments of the same software version on the same platform share identical credentials. This flaw allows unauthenticated remote attackers to compromise cloud-based Cisco ISE instances and perform unauthorized administrative actions, potentially leading to the exposure of sensitive data, system misconfiguration, or service disruption.

This vulnerability does not affect on-premises deployments or hybrid deployments where the Primary Administration node is on-premises.

There are no workarounds, but Cisco has released hotfixes and patched versions to address this issue. All affected customers are strongly urged to update immediately.

Vulnerability Details:

- CVE ID: CVE-2025-20286
- CVSS Score: Base 9.9 CRITICAL
- Static credentials are improperly generated during cloud deployments of Cisco ISE, causing different instances to share the same admin-level credentials across identical software versions and platforms. This allows an attacker to:
  - Extract credentials from a compromised ISE cloud instance.
  - Reuse the same credentials to access other ISE instances on unsecured ports.
  - Perform administrative actions or disrupt services.

Affected Products:

Cloud Platform	Vulnerable Cisco ISE Versions
AWS	3.1, 3.2, 3.3, 3.4
Azure	3.2, 3.3, 3.4
OCI	3.2, 3.3, 3.4

Fixed Releases:

Cisco ISE Release	Hot Fix	First Fixed Release
3.0 and earlier	Not applicable.	Not affected.
3.1	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz	Migrate to a fixed release.
	This hot fix applies to Releases 3.1 through 3.4.	

3.2	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz This hot fix applies to Releases 3.1 through 3.4.	Migrate to a fixed release.
3.3	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz This hot fix applies to Releases 3.1 through 3.4.	3.3P8 (November 2025)
3.4	ise-apply-CSCwn63400_3.1.x_patchall-SPA.tar.gz This hot fix applies to Releases 3.1 through 3.4.	3.4P3 (October 2025)
3.5	Not applicable.	Planned release (Aug 2025)

Mitigations:
Although no direct workarounds are available, the following mitigations are recommended:

- IP Whitelisting: Restrict access to Cisco ISE instances by source IP at both the cloud platform and within ISE's configuration.
- Credential Regeneration: For fresh installations, regenerate credentials using the application reset-config ise command.
- Backup Management: Ensure only post-patch backups are restored to avoid reverting to shared credential states.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to apply the relevant hotfix or upgrade to the fixed version if available.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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