Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco ISE Cloud Deployments Exposed to Remote Access Risk

Date of Publication	Admiralty Code	TA Number
June 6, 2025	A1	TA2025178

Summary

First Seen: June 4, 2025
Affected Product: Cisco ISE (Cloud Deployments)
Affected Platforms: AWS, Azure, OCI
Impact: CVE-2025-20286 is a critical vulnerability in Cisco ISE cloud deployments (AWS, Azure, OCI) due to shared static credentials across instances of the same version. It allows unauthenticated remote attackers to access, modify, or disrupt systems. Only cloud-based Primary Admin Nodes are affected; on-prem setups are safe. A public proof-of-concept exploit exists, increasing risk. Immediate patching and strict access controls are strongly recommended as there is no direct workaround.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-20286	Cisco Identity Services Engine Static Credential Vulnerability	Cisco Identity Services Engine on Cloud Platforms	☒	☒	✓

Vulnerability Details

#1 CVE-2025-20286 is a critical vulnerability affecting Cisco Identity Services Engine (ISE) when deployed in cloud environments such as Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI). The vulnerability stems from flawed credential generation during cloud deployment, causing identical static credentials to be assigned across all ISE instances using the same software version and cloud platform. For instance, all Cisco ISE 3.1 deployments on AWS would share the same default credentials, though these are not reused across differing releases or platforms.

#2 This flaw poses a severe security risk, allowing unauthenticated remote attackers to gain access to sensitive system data, perform limited administrative functions, and potentially modify configurations or disrupt services. Exploitation is only possible in deployments where the Primary Administration Node is hosted in the cloud; on-premises deployments are not affected.

#3

A PoC exploit is publicly available, increasing the risk of exploitation. Although there are no confirmed attacks in the wild yet, attackers could easily leverage the PoC to extract credentials from one instance and use them to access others, particularly if instances are exposed to the internet or lack proper access controls. Cisco users deploying ISE in the cloud should act immediately to secure their systems and reduce the risk of compromise, especially in environments where centralized identity management is critical to network security.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-20286	Cisco ISE versions: 3.1 to 3.4	cpe:2.3:a:cisco:identity_services_engine:3.0:*:*:*:*:*:*:*	CWE-259

Recommendations

Upgrade to Patched Versions: Apply the latest security patches or hotfixes for Cisco ISE versions 3.1 to 3.4 as soon as they are available.

Restrict Administrative Access: Limit access to the ISE administrative interfaces to trusted IP addresses only, using firewall rules or access control lists (ACLs).

Regenerate Credentials for New Installations: For fresh deployments, use the application reset-config ise command to regenerate unique credentials, note this resets the system to factory defaults.

Avoid Restoring Vulnerable Backups: Ensure backups do not reintroduce shared credentials; test and validate backup integrity after patching.

Monitor and Audit: Continuously monitor for unauthorized access or unusual administrative activity, and audit systems for exposure to this vulnerability.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0006 Credential Access	**T1588** Obtain Capabilities	**T1588.005** Exploits	**T1078.001** Default Accounts
T1552 Unsecured Credentials	**T1190** Exploit Public-Facing Application	**T1078** Valid Accounts	**T1588.006** Vulnerabilities

Patch Link

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

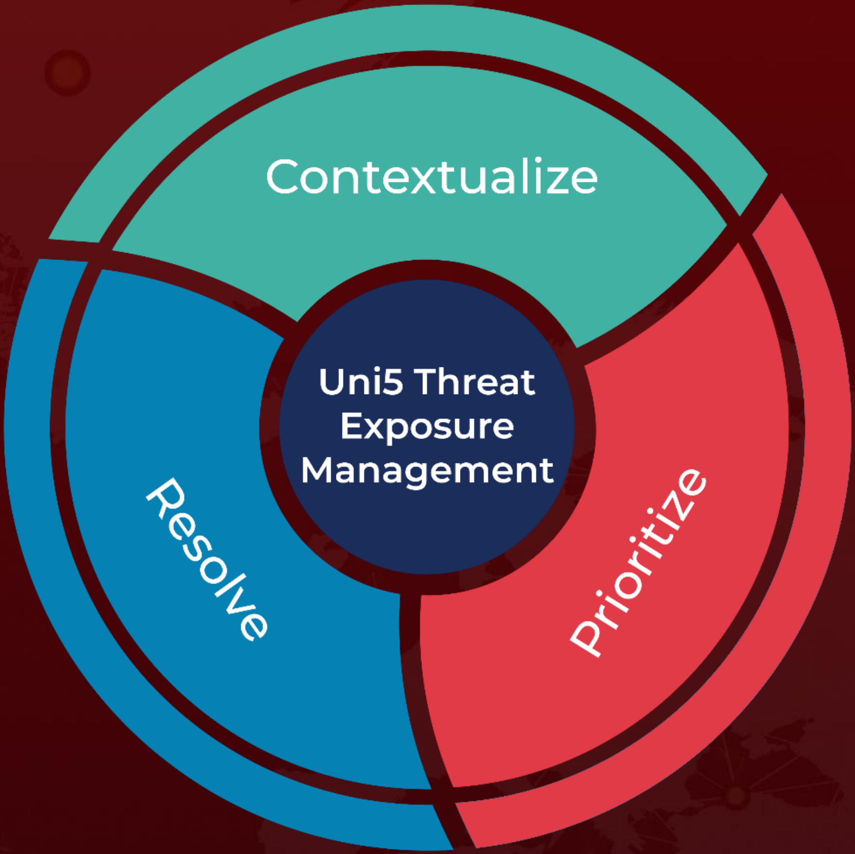
References

https://digital.nhs.uk/cyber-alerts/2025/cc-4664

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 6, 2025 • 7:30 AM

More at www.hivepro.com