Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Critical Cisco ISE Flaws Actively Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
July 23, 2025	A1	TA2025229

Summary

First Seen: June 2025
Affected Product: Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC)
Impact: Three recently patched critical vulnerabilities in Cisco Identity Services Engine (ISE), tracked as CVE-2025-20281, CVE-2025-20282, and CVE-2025-20337, affect Cisco ISE and its Passive Identity Connector (ISE-PIC), a platform used by organizations to control network access and enforce security policies. Two of the vulnerabilities allow unauthenticated remote attackers to gain root-level access by sending specially crafted API requests, while the third allows malicious files to be uploaded into sensitive system directories for remote code execution. Some of these flaws are now being actively exploited in the wild, and users are urged to update to the fixed versions immediately, as exploitation attempts have already been observed since July 2025.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-20281	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability	Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC)	✗	✗	✓
CVE-2025-20282	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability		✗	✗	✓
CVE-2025-20337	Cisco ISE API Unauthenticated Remote Code Execution Vulnerability		✗	✗	✓

Vulnerability Details

#1 Cisco has sounded the alarm on three critical vulnerabilities, CVE-2025-20281, CVE-2025-20282, and CVE-2025-20337 some of which are now being actively exploited in the wild. These flaws affect the widely deployed Cisco Identity Services Engine (ISE), a core solution used by enterprises to enforce network access policies, authenticate users and devices, and manage segmentation. The vulnerabilities also impact ISE-PIC, a component that passively collects identity data from systems like Active Directory.

#2 Alarmingly, attackers do not need any credentials to exploit these flaws. CVE-2025-20281 and CVE-2025-20337 stem from weak input validation in a specific API, allowing unauthenticated remote attackers to send crafted requests and execute code on the system with root-level privileges. CVE-2025-20282, on the other hand, results from improper file validation enabling attackers to upload and run malicious files in sensitive system directories.

#3 These vulnerabilities are independent, meaning one doesn't rely on the other for exploitation. The exploitation attempts began in July 2025, highlighting the urgency for immediate action. Organizations relying on Cisco ISE or ISE-PIC are strongly advised to apply the latest security patches without delay to avoid potential compromise.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-20281	Cisco ISE and ISE-PIC releases 3.3 and 3.4	cpe:2.3:a:cisco:identity_services_engine:*:*:*:*:*:*:* cpe:2.3:a:cisco:identity_services_engine_passive_identity_connector:*:*:*:*:*:*:*	CWE-74
CVE-2025-20282	Cisco ISE and ISE-PIC Release 3.4		CWE-269
CVE-2025-20337	Cisco ISE and ISE-PIC releases 3.3 and 3.4		CWE-74

Recommendations

- **Update Immediately:** Install the latest security patches for Cisco ISE and ISE-PIC as soon as possible. These vulnerabilities are already being used by attackers in the wild, so delaying updates could leave your systems wide open.
- **Check for Unusual Activity:** Review system logs for any unexpected API activity, unknown file uploads, or unusual root-level access attempts. These may be signs that an attacker has already tried to exploit your system.
- **Limit External Access to Admin Interfaces:** Make sure your Cisco ISE management interfaces are not accessible from the open internet. Use a VPN or trusted network to access these tools whenever possible.
- **Back Up Configurations:** Back up your ISE configurations before applying updates. This ensures you can quickly restore your settings if anything goes wrong during the patch process.
- **Vulnerability Management:** This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0004 Privilege Escalation	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter	T1068 Exploitation for Privilege Escalation	T1203 Exploitation for Client Execution

Patch Details

Install the latest version of Cisco ISE and ISE-PIC to address the flaws.
ISE 3.3 upgrade to Patch 7
ISE 3.4 upgrade to Patch 2
ISE 3.2 or earlier are not affected

Link:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

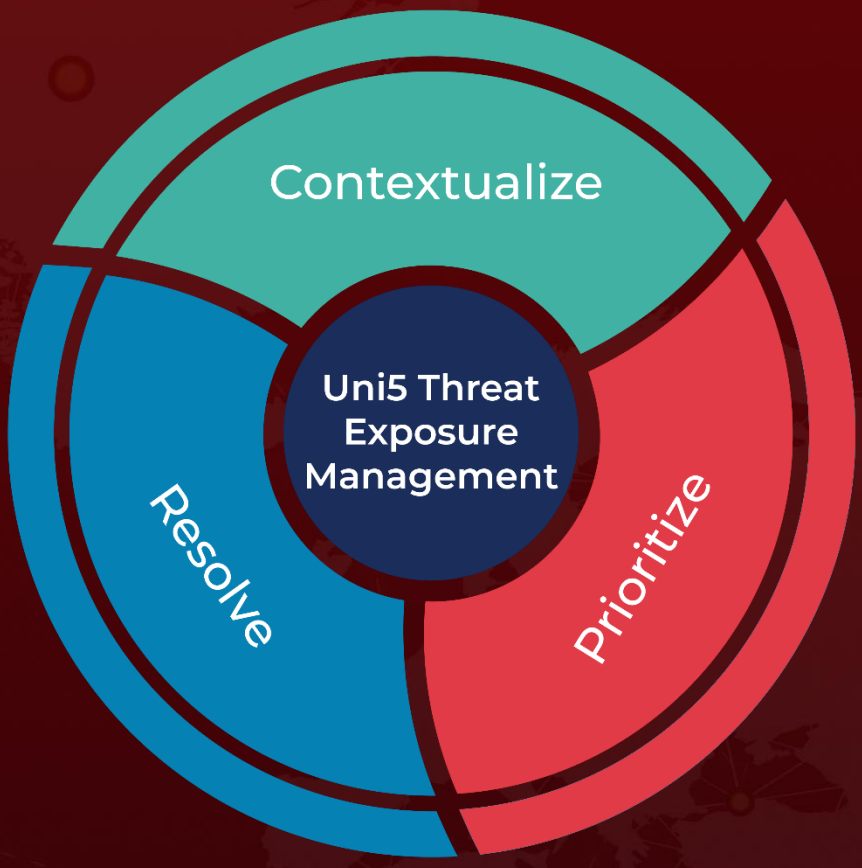
References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

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

July 23, 2025 • 6:00 AM

More at www.hivepro.com