Cisco Identity Services Engine (Ise) Java Deserialization And Authorization Vulnerabilities

Vairav Advisory Report

Date: February 06, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

CVE-2025-20124 and CVE-2025-20125 are critical vulnerabilities affecting Cisco Identity Services Engine (ISE) software. CVE-2025-20124 is a Java deserialization vulnerability that allows an authenticated, remote attacker to execute arbitrary commands as the root user on an affected device. CVE-2025-20125 is an authorization flaw in an API of Cisco ISE that permits an attacker to obtain sensitive information, modify node configurations, and restart the node. Both vulnerabilities require valid read-only administrative credentials for exploitation. Cisco has released patches to address these issues, and users are strongly advised to update their systems immediately.

VULNERABILITY DETAILS

CVE-2025-20124

Description: A Java deserialization vulnerability in Cisco ISE allows an authenticated, remote attacker to execute arbitrary commands as the root user by sending a crafted serialized Java object to an affected API.

Impact: Unauthorized command execution, privilege escalation.

CVSS Score: 9.9 (Critical)

AFFECTED VERSIONS:

Cisco Identity Services Engine Software:

- 3.0.0, 3.0.0 p1, 3.0.0 p2, 3.0.0 p3, 3.0.0 p4, 3.0.0 p5, 3.0.0 p6, 3.0.0 p7, 3.0.0 p8
- 3.1.0, 3.1.0 p1, 3.1.0 p2, 3.1.0 p3, 3.1.0 p4, 3.1.0 p5, 3.1.0 p6, 3.1.0 p7, 3.1.0 p8, 3.1.0 p9
- 3.2.0, 3.2.0 p1, 3.2.0 p2, 3.2.0 p3, 3.2.0 p4, 3.2.0 p5, 3.2.0 p6
- 3.3.0, 3.3 Patch 1, 3.3 Patch 2, 3.3 Patch 3
- 2.7.0 p8

CVE-2025-20125

Description: An authorization flaw in Cisco ISE allows an authenticated, remote attacker to obtain sensitive information, modify system configurations, and restart the node by sending a crafted HTTP request to a specific API.

Impact: Information disclosure, unauthorized configuration modification, denial-of-service (DoS).

CVSS Score: 9.1 (Critical)

AFFECTED VERSIONS:

Cisco Identity Services Engine Software:

- 3.0.0, 3.0.0 p1, 3.0.0 p2, 3.0.0 p3, 3.1.0, 3.0.0 p4, 3.1.0 p1, 3.0.0 p5, 3.1.0 p3, 3.1.0 p2
- 3.0.0 p6, 3.2.0, 3.1.0 p4, 2.7.0 p8, 3.1.0 p5, 3.2.0 p1, 3.0.0 p7, 3.1.0 p6, 3.2.0 p2, 3.1.0 p7
- 3.3.0, 3.2.0 p3, 3.0.0 p8, 3.2.0 p4, 3.1.0 p8, 3.2.0 p5, 3.2.0 p6, 3.1.0 p9, 3.3 Patch 2, 3.3 Patch 1, 3.3 Patch 3

Cisco ISE Passive Identity Connector:

- 3.0.0, 3.1.0, 3.2.0, 3.3.0

Cisco ISE Passive Identity Connector: 3.0.0, 3.1.0, 3.2.0, 3.3.0

EXPLOIT DETAILS

These vulnerabilities can be exploited by sending specially crafted network requests to vulnerable Cisco ISE APIs. Successful exploitation may allow privilege escalation, system modifications, or denial-of-service attacks.

RECOMMENDED ACTIONS

- Cisco has released patches to mitigate these vulnerabilities. Users should upgrade to the latest available versions of their affected products.

ADDITIONAL SECURITY MEASURES

- Limit the use of Java deserialization and enforce strict authorization policies.
- Restrict network access to administrative interfaces.

REFERENCES

https://www.cve.org/CVERecord?id=CVE-2025-20124

https://www.cve.org/CVERecord?id=CVE-2025-20125

https://nvd.nist.gov/vuln/detail/CVE-2025-20125

https://nvd.nist.gov/vuln/detail/CVE-2025-20124

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multivuls-FTW9AOXF

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com