NATIONAL CSIRT-CY

CVE-2025-20125 / CVE-2025-20124 **06/02/2025**

CVE-2025-20124: Cisco ISE Insecure Java Deserialization Vulnerability

CVE-2025-20125: Cisco ISE Authorization Bypass Vulnerability

Description

CVE-2025-20124: Cisco ISE Insecure Java Deserialization Vulnerability

A vulnerability in an API of Cisco ISE could allow an authenticated, remote attacker to execute arbitrary commands as the *root* user on an affected device.

CVE-2025-20125: Cisco ISE Authorization Bypass Vulnerability

A vulnerability in an API of Cisco ISE could allow an authenticated, remote attacker with valid read-only credentials to obtain sensitive information, change node configurations, and restart the node.

Analysis

CVE-2025-20124

This vulnerability is due to insecure deserialization of user-supplied Java byte streams by the affected software. An attacker could exploit this vulnerability by sending a crafted serialized Java object to an affected API. A successful exploit could allow the attacker to execute arbitrary commands on the device and elevate privileges.

Note: To successfully exploit this vulnerability, the attacker must have valid read-only administrative credentials. In a single-node deployment, new devices will not be able to authenticate during the reload time.

CVE-2025-20125

This vulnerability is due to a lack of authorization in a specific API and improper validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted HTTP request to a specific API on the device. A successful exploit could allow the attacker to attacker to obtain information, modify system configuration, and reload the device.

Note: To successfully exploit this vulnerability, the attacker must have valid read-only administrative credentials. In a single-node deployment, new devices will not be able to authenticate during the reload time.

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/502.html
https://cwe.mitre.org/data/definitions/285.html

Common Vulnerabilities & Exposures

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

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

Solutions

Upgrade to an appropriate fixed software release as indicated in this section.

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

Cisco ISE Software Releases	***First Fixed Release***
3.0	*Migrate to a fixed release.*
3.1	*3.1P10*
3.2	*3.2P7*
3.3	*3.3P4*
3.4	*Not vulnerable.*

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.