Security Advisory 2025-025

Critical Vulnerabilities in Cisco ISE

2025-07-18 — v1.0

TLP:CLEAR

History:

- *18/07/2025 — v1.0 – Initial publication*

Summary

On June 25, Cisco released an advisory addressing 2 critical vulnerabilities affecting Cisco's Identity Services Engine (ISE) product that would allow an attacker to execute arbitrary code on vulnerable devices [1].

On July 16, Cisco updated this advisory adding a third critical vulnerability affecting Cisco's Identity Services Engine (ISE) product [1].

It is recommended updating affected product as soon as possible.

Technical Details

The vulnerabilities **CVE-2025-20281** and **CVE-2025-20337**, both with a CVSS score of 10, are due to insufficient validation of user-supplied input in a specific API endpoint of the product. An attacker could exploit these vulnerabilities by submitting a crafted API request. A successful exploit could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root.

The vulnerability **CVE-2025-20282**, with a CVSS score of 10, is due to a lack of file validation checks that would prevent uploaded files from being placed in privileged directories on an affected system. An attacker could exploit this vulnerability by uploading a crafted file to the affected device. A successful exploit could allow the attacker to store malicious files on the affected system and then execute arbitrary code or obtain root privileges on the system.

Affected Products

The following product versions are affected by the vulnerabilities:

- Cisco ISE or ISE-PIC Release 3.3 before Patch 7
- Cisco ISE or ISE-PIC Release 3.4 before Patch 2

Note: Cisco warns that customers who applied the patches for CVE-2025-20281 and CVE-2025-20282 are not covered for CVE-2025-20337, and need to upgrade to ISE 3.3 Patch 7 or ISE 3.4 Patch 2.

Recommendations

It is recommended updating affected devices as soon as possible.

References

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