CISCO ISE/ISE-PIC: TWO CRITICAL REMOTE CODE EXECUTION VULNERABILITIES (CVE-2025-20281 & CVE-2025-20282)

Vairav CVE Report

Date: June 27, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

Cisco has released a critical advisory for two zero-authentication Remote Code Execution (RCE) vulnerabilities, CVE-2025-20281 and CVE-2025-20282, affecting Cisco Identity Services Engine (ISE) and Passive Identity Connector (ISE-PIC). Both vulnerabilities carry a CVSS score of 10.0, indicating maximum severity. Exploitation of either flaw allows unauthenticated attackers to execute arbitrary commands with root privileges, leading to full system compromise. Immediate patching is strongly recommended.

VULNERABILITY DETAILS

CVE-2025-20281: API Input Validation Bypass

Description: Insufficient input validation in a specific API of Cisco ISE and ISE-PIC (version 3.3 and later) allows unauthenticated remote attackers to send crafted API requests, resulting in arbitrary code execution as root.

Impact: Remote Code Execution (RCE) with root privileges

CVSS Score: 10.0 (Critical)

Affected Products and Versions: Cisco ISE and ISE-PIC 3.3 and later

Exploit Details: Exploitation does not require authentication; attackers can remotely submit crafted requests to exploit the flaw.

CVE-2025-20282: Insecure File Upload in Internal API

Description: An internal API in Cisco ISE and ISE-PIC version 3.4 lacks validation on uploaded files, enabling unauthenticated attackers to upload malicious files to sensitive directories and execute them with root privileges.

Impact: Arbitrary File Upload and Code Execution as root

CVSS Score: 10.0 (Critical)

Affected Products and Versions: Cisco ISE and ISE-PIC 3.4 only

Exploit Details: No authentication required. Attackers can place and execute malicious files in privileged paths.

AFFECTED PRODUCTS/VERSIONS

- CVE-2025-20281: Cisco ISE and ISE-PIC 3.3 and later

- **CVE-2025-20282:** Cisco ISE and ISE-PIC 3.4 only

RECOMMENDED ACTIONS

- **Immediate Patching:**
  - Apply Patch 6 for Cisco ISE 3.3 (for CVE-2025-20281)
  - Apply Patch 2 for Cisco ISE 3.4 (for CVE-2025-20282)
- **Restrict Network Access:** Temporarily limit exposure of affected API endpoints where feasible until patching is complete.
- **Monitor for Exploitation:** Use intrusion detection systems to flag suspicious API activity or unexpected file uploads.
- **Audit Systems:** Check system logs for unusual access patterns or signs of post-exploitation activity.

REFERENCES

https://securityonline.info/cisco-ise-ise-pic-alert-two-critical-rce-flaws-cvss-10-0-allow-unauthenticated-root-access/

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

https://www.cve.org/CVERecord?id=CVE-2025-20281

https://www.cve.org/CVERecord?id=CVE-2025-20282

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: sales@vairavtech.com

Website: https://vairavtech.com

VAIRAV TECH
CYBER DEFENDER