Computer Emergency Response Team of Mauritius

A department under the Ministry of Information Technology, Communication and Innovation

CERT-MU Security Advisory

CERT-MU Advisories AD-2025-04

Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities

Date of Issue: 29 July 2025

Severity Rating: High

Systems Affected:

- Cisco ISE and ISE-PIC releases 3.3 and 3.4
- Cisco ISE and ISE-PIC Release 3.4

CVE Information:

- CVE-2025-20281
- CVE-2025-20337
- CVE-2025-20282

Description

Multiple vulnerabilities have been identified Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) and they could be exploited to allow an unauthenticated, remote attacker to issue commands on the underlying operating system as the root user.

Technical details

CVE-2025-20281 and CVE-2025-20337: Cisco ISE API Unauthenticated Remote Code Execution Vulnerabilities

Multiple vulnerabilities in a specific API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to execute arbitrary code on the underlying operating system as root. The attacker does not require any valid credentials to exploit these vulnerabilities.

These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.

CVE-2025-20282: Cisco ISE API Unauthenticated Remote Code Execution Vulnerability

A vulnerability in an internal API of Cisco ISE and Cisco ISE-PIC could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device and then execute those files on the underlying operating system as root.

This vulnerability is due 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.

Workarounds
There are no workarounds that address these vulnerabilities.

Fixed Software
Cisco has released free software updates that address the vulnerability. Customers with service contracts that entitle them to regular software updates should obtain security fixes through their usual update channels.

More information is available on:
https://sec.cloudapps.cisco.com/security/center/resources/security_vulnerability_policy.html#ssu

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

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,