Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Cisco Identity Services Engine Unauthenticated Remote Code Execution Vulnerabilities

Vulnerability Note: VN-2025-05

Date of Issue: 25 June 2025

Severity Rating: High

Systems Affected:

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

Description

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

1. CVE-2025-20281: Cisco ISE API Unauthenticated Remote Code Execution Vulnerability

A vulnerability 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 this vulnerability. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted API request. A successful exploit could allow the attacker to obtain root privileges on an affected device.

2. 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.

Solution

Cisco has released software updates that address the vulnerability described in this advisory. More information is available on:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

CVE Information
CVE-2025-20281
CVE-2025-20282

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,