

Date Posted: 2025/06/30

[Vulnerability Alert] Critical Security Vulnerabilities in Cisco Identity Services

- Subject: [Vulnerability Alert] Critical Security Vulnerabilities in Cisco Identity Services
- Content Description:
 - Forwarded from Taiwan Computer Emergency Response Team/Coordination Center TWCERTCC-200-202506-00000018
 - Cisco Identity Services Engine (ISE) is an identity-based security management platform that collects information from networks and user devices, and enforces policies and makes regulatory decisions within the network infrastructure. Cisco recently issued a major security vulnerability announcement (CVE-2025-20281, CVSS: 9.8 and CVE-2025-20282, CVSS: 10.0) and released updated versions.
 - [CVE-2025-20281, CVSS: 9.8] This vulnerability exists in specific APIs of Cisco ISE and Cisco ISE-PIC, allowing unauthenticated remote attackers to execute arbitrary code as root on the underlying operating system without any valid credentials.
 - [CVE-2025-20282, CVSS: 10.0] This vulnerability exists in the internal API of Cisco ISE and Cisco ISE-PIC, allowing unauthenticated remote attackers to upload arbitrary files to the affected device and execute them as root on the underlying operating system.
- Affected Platforms:
 - [CVE-2025-20281] Cisco ISE and ISE-PIC versions 3.3, 3.4
 - [CVE-2025-20282] Cisco ISE and ISE-PIC version 3.4
- Suggested Measures:
 - Please apply patches according to the solutions released on the official website:
<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2Gnj6>
- References:
 1. <https://www.twcert.org.tw/tw/cp-169-10220-062b3-1.html>

Computer and Communications Center
Network Systems Division Respectfully

From:

<https://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

https://net.nthu.edu.tw/netsys/en:mailing:announcement:20250630_03



Last update: **2025/06/30 09:53**