Posted Date: 2026/04/30

Vulnerability Alert Three Critical Security Vulnerabilities in Cisco Identity Services Engine

- Subject: Vulnerability Alert Three Critical Security Vulnerabilities in Cisco Identity Services Engine

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202604-00000018
  - Cisco Identity Services Engine (ISE) is an identity-based security management platform that gathers information from networks and user devices to implement policies and make regulatory decisions across network infrastructure. Cisco recently issued a major security vulnerability announcement.
  - CVE-2026-20180, CVSS: 9.9 and CVE-2026-20186, CVSS: 9.9 Both are Remote Code Execution (RCE) vulnerabilities, allowing authenticated remote attackers to execute arbitrary commands on the underlying operating system of the affected device.
  - To exploit these vulnerabilities, the attacker must possess at least read-only administrator privileges.
  - CVE-2026-20147, CVSS: 9.9 This vulnerability allows authenticated remote attackers to execute arbitrary commands on the underlying operating system of the affected device. Successful exploitation requires the attacker to possess at least valid administrator credentials.
- Affected Platforms:
  - Cisco ISE 3.2 and earlier versions
  - Cisco ISE 3.2
  - Cisco ISE 3.3
  - Cisco ISE 3.4
  - Cisco ISE or Cisco ISE-PIC 3.1 and earlier versions
  - Cisco ISE or Cisco ISE-PIC 3.2
  - Cisco ISE or Cisco ISE-PIC 3.3
  - Cisco ISE or Cisco ISE-PIC 3.4
  - Cisco ISE or Cisco ISE-PIC 3.5
- Recommended Actions:
  - Please update to the following versions:
  - CVE-2026-20180, CVE-2026-20186 Cisco ISE 3.2 Patch 8, Cisco ISE 3.3 Patch 8, Cisco ISE 3.4 Patch 5
  - CVE-2026-20147 Cisco ISE or Cisco ISE-PIC 3.1 Patch 11, Cisco ISE or Cisco ISE-PIC 3.2 Patch 10, Cisco ISE or Cisco ISE-PIC 3.3 Patch 11, Cisco ISE or Cisco ISE-PIC 3.4 Patch 6, Cisco ISE or Cisco ISE-PIC 3.5 Patch 3
  - Note: Cisco ISE-PIC has reached End-of-Sale; version 3.4 is the last supported version.
- Reference:
  1. https://www.twcert.org.tw/tw/cp-169-10849-9d3d6-1.html

Computer and Communication Center
Network Systems Division

From:
https://net.nthu.edu.tw/netsys/ - **網路系統組**

Permanent link:
https://net.nthu.edu.tw/netsys/en:mailing:announcement:20260430_21

Last update: **2026/04/30 08:44**