**Date Posted: 2026/08/07**

# Vulnerability AlertTwo Critical Security Vulnerabilities in Cisco IOS XE Software

- Subject: Vulnerability AlertTwo Critical Security Vulnerabilities in Cisco IOS XE Software

- Description:
  - Forwarded Security Alert from TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) TWCERTCC-200-202608-00000004
  - The Cisco IOS XE software development team discovered multiple security vulnerabilities during an internal security review and has completed the patches. Currently, there is no evidence indicating that these vulnerabilities have been actively exploited. To assist customers in deploying security updates in a timely manner and to streamline the disclosure process, Cisco has publicly disclosed the relevant vulnerability details and remediation guidance. CVE-2026-20267 (CVSS: 9.0) is an improper access control vulnerability; CVE-2026-20272 (CVSS: 9.8) is an improper neutralization of special elements vulnerability.
- Affected Platforms:
  - Cisco IOS XE 17.9, Cisco IOS XE 17.12, Cisco IOS XE 17.15, Cisco IOS XE 17.18, Cisco IOS XE 26.1
- Recommendations:
  - Please update to the following versions or later: Cisco IOS XE 17.12.18, Cisco IOS XE 17.15.6, Cisco IOS XE 17.18.4, Cisco IOS XE 17.18.4a, Cisco IOS XE 26.1.2
- Reference Information:
  1. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-20267
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-20272

---

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:20260807_24**

Last update: **2026/08/07 09:56**