

Date Posted: 2026/08/07

□Vulnerability Alert□Four Critical Security Vulnerabilities in Cisco Catalyst SD-WAN

- Subject: □Vulnerability Alert□Four Critical Security Vulnerabilities in Cisco Catalyst SD-WAN
- Description:
 - Forwarded Security Alert from TWCERT/CC (Taiwan Computer Emergency Response Team/Coordination Center) TWCERTCC-200-202608-00000005
 - Cisco Catalyst SD-WAN is Cisco's cloud-centric software-defined WAN architecture, providing centralized management, secure encryption, and application performance optimization to ensure reliable connectivity in multi-cloud environments. The Catalyst SD-WAN 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-2026-20303 (CVSS: 9.9) is an improper input validation vulnerability; CVE-2026-20304 (CVSS: 9.9) is an improper access control vulnerability; CVE-2026-20310 (CVSS: 9.9) is an incorrect link resolution before file access vulnerability; CVE-2026-20312 (CVSS: 8.8) is a storage of sensitive information in plaintext vulnerability.
- Affected Platforms:
 - Cisco Catalyst SD-WAN 20.9 and prior, Cisco Catalyst SD-WAN 20.10, Cisco Catalyst SD-WAN 20.11, Cisco Catalyst SD-WAN 20.12, Cisco Catalyst SD-WAN 20.13, Cisco Catalyst SD-WAN 20.14, Cisco Catalyst SD-WAN 20.15, Cisco Catalyst SD-WAN 20.16, Cisco Catalyst SD-WAN 20.18, Cisco Catalyst SD-WAN 26.1
- Recommendations:
 - Please update to the following versions or later: Cisco Catalyst SD-WAN 20.9.10, Cisco Catalyst SD-WAN 20.12.8.1, Cisco Catalyst SD-WAN 20.15.6, Cisco Catalyst SD-WAN 20.18.4, Cisco Catalyst SD-WAN 26.1.2
- Reference Information:
 1. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K>
 2. <https://nvd.nist.gov/vuln/detail/CVE-2026-20303>
 3. <https://nvd.nist.gov/vuln/detail/CVE-2026-20304>
 4. <https://nvd.nist.gov/vuln/detail/CVE-2026-20310>
 5. <https://nvd.nist.gov/vuln/detail/CVE-2026-20312>

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_25



Last update: **2026/08/07 10:02**