Post Date: 2026/05/19

Vulnerability Alert Critical Security Vulnerability in Cisco Catalyst SD-WAN (CVE-2026-20182)

- Subject: Vulnerability Alert Critical Security Vulnerability in Cisco Catalyst SD-WAN (CVE-2026-20182)

- Description:
  - Forwarded from Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Advisory TWCERTCC-200-202605-00000011
  - Cisco Catalyst SD-WAN is Cisco's cloud-centric software-defined wide area network architecture that provides centralized management, secure encryption, and application performance optimization to ensure reliable connectivity across multi-cloud environments. Cisco has recently released a critical security advisory.
  - CVE-2026-20182, CVSS: 10.0 This vulnerability exists in the Cisco Catalyst SD-WAN Controller (formerly vSmart) and Catalyst SD-WAN Manager (formerly vManage). It allows a remote attacker to send crafted requests to bypass authentication and obtain internal high-privileged accounts (non-root).
  - Attackers can subsequently leverage these high-privileged accounts to access NETCONF, modify the SD-WAN network architecture configuration, establish malicious network nodes, and conduct further deep attacks on enterprise/organizational networks.
  - Note: Active exploitation in the wild has been observed targeting Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage). Please take immediate response measures.
- Affected Platforms:
  - Cisco Catalyst SD-WAN On-Prem Deployment, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed), Cisco SD-WAN for

Government (FedRAMP)

- Recommended Actions:
  - Apply patches according to the solutions released on the official website: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

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:20260519_21

Last update: **2026/05/19 11:17**