Date Posted: 2026/03/03

[Vulnerability Alert] 3 Critical Security Vulnerabilities Found in Cisco Catalyst SD-WAN

- Subject Explanation: [Vulnerability Alert] 3 Critical Security Vulnerabilities Found in Cisco Catalyst SD-WAN

- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202602-00000014
  - Cisco Catalyst SD-WAN is a cloud-centric software-defined wide area network architecture by Cisco that provides centralized management, secure encryption, and application performance optimization to ensure reliable connections in multi-cloud environments. Recently, Cisco released a critical security advisory.
  - [CVE-2026-20127, CVSS: 10.0] This vulnerability exists in the Cisco Catalyst SD-WAN Controller (formerly vSmart) and may be exploited by an unauthenticated remote attacker to bypass the authentication mechanism and gain administrative privileges on the affected system.
  - [CVE-2026-20126, CVSS: 8.8] This vulnerability exists in the Cisco Catalyst SD-WAN Manager (formerly vManage) and may allow an authenticated attacker with low local privileges to send a request via the REST API to obtain root privileges on the underlying operating system.
  - [CVE-2026-20129, CVSS: 9.8] This vulnerability exists in the API user authentication of the Cisco Catalyst SD-WAN Manager. It allows an unauthenticated remote attacker to use a carefully crafted API request to access the affected system as a user with the netadmin role. Note: The Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage) have been found to be actively exploited in attack campaigns; please take responsive measures immediately.
- Impacted Platforms:
  - [CVE-2026-20127]
  - Cisco Catalyst SD-WAN 20.9 version, Cisco Catalyst SD-WAN 20.11 version, Cisco Catalyst SD-WAN 20.12.5 version, Cisco Catalyst SD-WAN 20.12.6 version, Cisco Catalyst SD-WAN 20.13 version, Cisco Catalyst SD-WAN 20.14 version, Cisco Catalyst SD-WAN 20.15 version, Cisco Catalyst SD-WAN 20.16 version, Cisco Catalyst SD-WAN 20.18 version
  - [CVE-2026-20126, CVE-2026-20129]
  - Cisco Catalyst SD-WAN Manager 20.9 version, Cisco Catalyst SD-WAN Manager 20.11 version, Cisco Catalyst SD-WAN Manager 20.12.5 version, Cisco Catalyst SD-WAN Manager 20.126 version, Cisco Catalyst SD-WAN Manager 20.13 version, Cisco Catalyst SD-WAN Manager 20.14 version, Cisco Catalyst SD-WAN Manager 20.15 version, Cisco Catalyst SD-WAN Manager 20.16 version, Cisco Catalyst SD-WAN Manager 20.18 version
- Suggested Measures:
  - Please update to the following versions:
  - [CVE-2026-20127]
  - Cisco Catalyst SD-WAN 20.9.8.2 and later versions

    - Cisco Catalyst SD-WAN 20.12.6.1 and later versions
    - Cisco Catalyst SD-WAN 20.12.5.3 and later versions
    - Cisco Catalyst SD-WAN 20.12.6.1 and later versions
    - Cisco Catalyst SD-WAN 20.15.4.2 and later versions
    - Cisco Catalyst SD-WAN 20.18.2.1 and later versions
    - [CVE-2026-20126, CVE-2026-20129]
    - Cisco Catalyst SD-WAN Manager 20.9.8.2 and later versions
    - Cisco Catalyst SD-WAN Manager 20.12.6.1 and later versions
    - Cisco Catalyst SD-WAN Manager 20.12.5.3 and later versions
    - Cisco Catalyst SD-WAN Manager 20.12.6.1 and later versions
    - Cisco Catalyst SD-WAN Manager 20.15.4.2 and later versions
    - Cisco Catalyst SD-WAN Manager 20.18.2.1 and later versions
- References:
    1. https://www.twcert.org.tw/tw/cp-169-10737-2a2d2-1.html

---

Computer and Communication Center
Network Systems Division