مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Vulnerabilities in Cisco Catalyst SD-WAN

Tracking #:432318462

Date:26-02-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical authentication bypass vulnerability, CVE-2026-20127, affecting Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager is being actively exploited in the wild.

TECHNICAL DETAILS:

A critical authentication bypass vulnerability, **CVE-2026-20127**, affecting Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager is being actively exploited in the wild. The flaw enables unauthenticated remote attackers to gain administrative access to affected systems.
Threat actors have been observed leveraging this vulnerability for initial access, followed by software downgrade attacks and subsequent privilege escalation via **CVE-2022-20775**, ultimately achieving root-level command execution.

Technical Details

1. **CVE-2026-20127 — CriticalAuthentication Bypass**
   - **Affected Products:** Cisco Catalyst SD-WAN Controller, Cisco Catalyst SD-WAN Manager
   - **Vulnerability Type:** Authentication Bypass
   - CVSS Score: Base 10.0
   - **Attack Vector:** Remote, unauthenticated
   - **Impact:** Full administrative access to the affected system without credentials
   - **CVSS Score:** Critical
   - **Disclosure Date:** February 25, 2026
   - **Exploitation Status:** Actively exploited in the wild

2. **CVE-2022-20775 — Privilege Escalation (Chained in Active Attacks)**
   - **Advisory ID:** cisco-sa-sd-wan-priv-E6e8tEd
   - **CVSS Score:** Base 7.8 (High) — CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
   - **Affected Products:** SD-WAN vBond Orchestrator Software, SD-WAN vEdge Cloud Routers, SD-WAN vEdge Routers, SD-WAN vManage Software, SD-WAN vSmart Controller Software
   - **Vulnerability Type:** Improper access controls on CLI commands (CWE-25)
   - **Attack Vector:** Local, authenticated attacker
   - **Impact:** Arbitrary command execution as the root user
   - **Exploitation Status:** Actively exploited in February 2026 as part of chained attack sequence

ATTACK CHAIN ANALYSIS

Threat actors observed in the wild are executing a deliberate multi-stage attack sequence:

1. **Initial Access** — Attackers exploit CVE-2026-20127 to bypass authentication and gain unauthenticated administrative access to the Cisco Catalyst SD-WAN Controller or Manager.
2. **Version Downgrade** — Once inside, attackers deliberately downgrade the software version on the compromised system to an older, vulnerable firmware release.
3. **Privilege Escalation** — With the system now running vulnerable older firmware, attackers exploit CVE-2022-20775 via the application CLI to execute arbitrary commands and escalate to full root access.

4. **Post-Exploitation** — With root access achieved, attackers have complete control of the SD-WAN infrastructure, including the ability to manipulate network routing, intercept traffic, establish persistence, and move laterally.

Patch Guidance for CVE-2026-20127

Upgrade to the following fixed releases based on your current major version:

- **20.9 Release** — Upgrade to 20.9.8.2 or above *(patch estimated available February 27, 2026)*
- **20.11 Release** — Upgrade to 20.12.6.1 or above
- **20.12.5 Release** — Upgrade to 20.12.5.3 or above
- **20.12.6 Release** — Upgrade to 20.12.6.1 or above
- **20.13 Release** — Upgrade to 20.15.4.2 or above
- **20.14 Release** — Upgrade to 20.15.4.2 or above
- **20.15 Release** — Upgrade to 20.15.4.2 or above
- **20.16 Release** — Upgrade to 20.18.2.1 or above
- **20.18 Release** — Upgrade to 20.18.2.1 or above
- **Releases below 20.9** — Migrate to a supported major version with an available fix

Patch Guidance for CVE-2022-20775 (Chained Exploit)

- **18.4 and earlier** — Migrate to a fixed release
- **19.2** — Migrate to a fixed release
- **20.3** — Migrate to a fixed release
- **20.6** — Upgrade to 20.6.3 or above
- **20.7** — Upgrade to 20.7.2 or above
- **20.8** — Upgrade to 20.8.1 or above
- **20.9** — Not affected

Detection and Forensic Guidance

Cisco recommends reviewing **control connection peering events** in Cisco Catalyst SD-WAN logs. All peering events must be manually validated using the following steps:

- **Verify timestamps** of each peering event against known maintenance windows, scheduled changes, and normal operational hours for your environment
- **Confirm the public IP address** of the peering event corresponds to infrastructure owned or authorized by your organization, cross-referenced against asset inventories and authorized IP ranges
- **Validate the peer system IP** matches documented device assignments within your Cisco Catalyst SD-WAN topology
- **Review the peer type** (vmanage, vsmart, vedge, vbond) to confirm it aligns with expected device roles in your deployment
- **Correlate multiple events** from the same source IP or system IP to identify patterns of reconnaissance or persistent access attempts
- **Cross-reference event timing** with authentication logs, change management records, and user activity to determine whether the connection was initiated by authorized personnel

RECOMMENDATIONS:

- Upgrade all affected SD-WAN systems to fixed versions.
- Block unauthorized management-plane access from the internet.
- Audit control-plane peering logs for anomalies.

- Disable unused administrative accounts.
- Rotate all SD-WAN administrative credentials.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk