مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Cisco Catalyst SD-WAN Manager

Tracking #:432319071

Date:05-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity privilege escalation vulnerability affecting Cisco Catalyst SD-WAN Manager is being actively exploited in limited cases. The vulnerability may allow authenticated attackers with sufficient privileges to execute arbitrary commands with root-level permissions through crafted file uploads.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-20245**
- **Severity:** High **CVSS:** 7.8
- The vulnerability exists due to insufficient validation of user-supplied input within the command-line interface (CLI) functionality of Cisco Catalyst SD-WAN Manager. A successful exploit allows attackers to perform command injection attacks and escalate privileges to the root user.
- To exploit this vulnerability, attackers require netadmin privileges on the affected system. Access may be obtained through valid credentials or by leveraging previously disclosed vulnerabilities, including CVE-2026-20182 or CVE-2026-20127.
- Cisco has observed limited exploitation activity where successful attacks resulted in unauthorized configuration changes being pushed to edge devices.

Affected Products

The vulnerability affects Cisco Catalyst SD-WAN Manager deployments regardless of configuration, including:

- On-Prem Deployment
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud (Cisco Managed)
- Cisco SD-WAN for Government (FedRAMP)

Indicators of Compromise (IoCs)

Review the following log file:

/var/log/scripts.log

Example suspicious log entry:

Apr 15 09:44:57 vmanage vScript: Tenant list upload per vsmart serial number: /usr/bin/vconfd_script_upload_tenant_list.sh -cli path /home/admin/malicious.csv vpn 0

Note: These commands may also appear during legitimate operations and should be evaluated against normal operational baselines.

Fixed Versions:

Cisco has not released software updates specifically addressing CVE-2026-20245 at the time of publication. Future software releases are expected to include remediation.

RECOMMENDATIONS:

- Identify and prioritize affected systems for assessment and remediation
- Preserve relevant logs and forensic artifacts before making changes
- Review systems for signs of unauthorized activity or configuration changes

- Restrict administrative access and enforce least-privilege principles
- Limit external exposure of management interfaces where possible
- Monitor systems for suspicious activity and unexpected behavior
- Apply vendor-provided updates and security fixes as soon as they become available
- Follow incident response procedures if compromise is suspected

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-sdwan-privesc-4uxFrdzx