Actively Exploited Cisco SD-WAN Zero-Day Enables Root Access and Unauthorized Configuration Changes

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

Cisco is warning organizations about active exploitation of CVE-2026-20245 (CVSS 7.8), a privilege escalation vulnerability affecting Cisco Catalyst SD-WAN Manager.

The vulnerability allows an attacker with netadmin privileges to execute commands as the root user. Cisco has also observed cases where exploitation resulted in configuration changes being pushed to managed SD-WAN edge devices. At this time, no patch is available.

Overview

There is a vulnerability in Cisco Catalyst SD-WAN Manager (formerly vManage) identified as CVE-2026-20245 (CVSS 7.8) that is being actively exploited by threat actors.

CVE-2026-20245 is caused by insufficient validation of user-supplied input within the SD-WAN Manager CLI. An attacker with netadmin privileges can upload a crafted file that triggers command injection and allows arbitrary commands to be executed as the root user.

Affected Products

The vulnerability affects Cisco Catalyst SD-WAN Manager across all deployment types:

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

Cisco has confirmed active exploitation in the wild and stated that some attacks resulted in configuration changes being pushed to managed SD-WAN edge devices.

This vulnerability is particularly concerning because attackers can obtain the required privileges by exploiting previously disclosed Cisco vulnerabilities, including CVE-2026-20182 and CVE-2026-20127, both of which have been exploited.

While this vulnerability does not directly affect firewalls, it impacts the platform used to manage Cisco SD-WAN environments. Cisco has observed cases where exploitation resulted in configuration changes being pushed to edge devices, which could affect network operations across the environment.

Aspire Protects

- **Patch** – Cisco has not released a software update for CVE-2026-20245 and there are currently no available workarounds. Organizations should focus on the following:
  - Determine whether Cisco Catalyst SD-WAN Manager is deployed within the environment.
  - Collect admin-tech files from all SD-WAN control components before performing upgrades or remediation activities.
  - Review /var/log/scripts.log for suspicious tenant upload activity.
  - Investigate recent or unexpected configuration changes pushed to SD-WAN edge devices.
  - Verify that routing, segmentation, and access control policies have not been modified without authorization.
  - Upgrade to the software releases that address CVE-2026-20182 and CVE-2026-20127.
  - Retain logs and admin-tech files before making changes to affected systems.
  - Monitor Cisco security advisories for future updates and the eventual release of a patch for CVE-2026-20245.

TTPs to Watch

Initial Access

- Valid Accounts [T1078] – The threat actor may use legitimate credentials to obtain netadmin access to Cisco Catalyst SD-WAN Manager.
- Exploit Public-Facing Application [T1190] – The threat actor may exploit previously disclosed SD-WAN vulnerabilities such as CVE-2026-20182 or CVE-2026-20127 to gain administrative access.

Execution

- Command and Scripting Interpreter [T1059] – The threat actor may upload a crafted file that allows arbitrary commands to be executed on the affected system.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Successful exploitation allows the threat actor to elevate privileges and execute commands as the root user.

Behavioral IoCs

- Unexpected tenant list uploads to vSmart controllers
- Configuration changes pushed to SD-WAN edge devices without authorization
- New or unusual netadmin account activity
- Administrative activity originating from unfamiliar IP addresses
- Tenant upload operations occurring outside approved maintenance windows
- Unauthorized changes to routing policies
- Unauthorized changes to network segmentation policies
- Unauthorized changes to access control policies
- Unusual file upload activity within Cisco Catalyst SD-WAN Manager

Technical IoCs

Log Artifacts

- `/var/log/scripts.log` (*Cisco recommends reviewing this log file*)
- `vconfd_script_upload_tenant_list.sh` (*script referenced in Cisco's example log entry*)

File Names

- `malicious.csv` (*example file name shown in Cisco's advisory*)

Example 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` (*activity Cisco recommends reviewing*)

Targeted Industries

Any organization using Cisco Catalyst SD-WAN Manager may be affected, including:

- Education
- Energy
- Finance
- Healthcare
- Legal
- Manufacturing
- Public Sector
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability

NVD - CVE-2026-20245