ADVISORY FOR ICM SECTOR

Threat Actor Exploits Network Management System for Privilege Escalation

Original report published on: June 25, 2026

Executive Summary

In June 2026, Mandiant (Google Cloud) publicly reported details of exploitation observed earlier in 2026 involving Cisco Catalyst SD-WAN at a service provider. During the intrusion, the threat actor exploited CVE-2026-20245 as a zero-day to escalate privileges and obtain root-level access to the compromised system. The vulnerability was disclosed by Cisco in June and was assigned a CVSS score of 7.8 (High). To exploit this vulnerability, an attacker must possess netadmin privileges or have already leveraged CVE-2026-20127 or CVE-2026-20182. By supplying a specially crafted file, the attacker can execute arbitrary commands as root.

The incident highlights the security risk associated with compromising centralised network management infrastructure. An attacker with elevated control of an SD-WAN management system may gain access to network configurations, establish persistence, and make configuration changes affecting connected edge devices. The investigation also identified efforts to remove evidence of the activity, underscoring the importance of preserving and examining forensic evidence.

Background

Cisco Catalyst SD-WAN provides centralised management and control of wide area network infrastructure. Its management components, including Catalyst SD-WAN Manager (formerly SD-WAN vManage), allow administrators to configure and manage distributed network devices. This centralised role makes the management plane a valuable target, as its compromise may provide access to sensitive network information and administrative functions.

CVE-2026-20245 is an authenticated privilege-escalation vulnerability affecting Cisco Catalyst SD-WAN Manager, Catalyst SD-WAN Controller (formerly SD-WAN vSmart) and Catalyst SD-WAN Validator (formerly SD-WAN vBond). An attacker with netadmin privileges can exploit the vulnerability by uploading a specially crafted file, enabling commands to be executed as root.

Two related critical vulnerabilities affecting the Cisco Catalyst SD-WAN Controller, CVE-2026-20127 and CVE-2026-20182, involve weaknesses in SD-WAN peering authentication and can allow an unauthenticated remote attacker to gain netadmin privileges. These vulnerabilities

could therefore provide the level of access required to subsequently exploit CVE-2026-20245.

Mandiant observed unauthorised peering activity during its investigation; however, the use of CVE-2026-20127 or CVE-2026-20182 was not conclusively established across the observed activity. After obtaining netadmin privileges, the attacker exploited CVE-2026-20245 to escalate privileges to root, accessed SD-WAN configuration information and attempted to remove evidence of the intrusion.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention against the exploitation of Cisco Catalyst SD-WAN Manager activity identified in this advisory:

- Ensure timely patching of Internet facing systems, including the upgrade of Cisco Catalyst SD-WAN Manager, Catalyst SD-WAN Controller and Catalyst SD-WAN Validator to fixed software releases.
- Scan for Indicators of Compromise to detect threat activities (Annex A), from logs and diagnostic data from Catalyst SD-WAN devices by executing *request admin-tech* command on all control-plane components.
- Monitor for unexpected root-equivalent accounts and validate against approved changes
- Establish alerting for suspicious peering, privileged sessions, CLI activity, uploads and configuration changes.
- Ensure privileged access controls and credential rotation following suspected exposure.
- Organisations should implement the comprehensive security best practices and configuration standards outlined in the Cisco Catalyst SD-WAN Hardening Guide which provides multi-layered defence across all Catalyst SD-WAN components—including management, control, and data planes—to prevent unauthorised access.

Annex A

Audit the *scripts.log* file, located at /var/log/, for entries that are shown in the following examples:

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
Jun 5 13:06:39 Manager vScript: vSmart upload serial numbers: /usr/bin/vconfd_script_upload_vsmart_serial_numbers.sh -cli path /home/admin/vsmart_serial_numbers_safe.csv
Jun 5 13:08:47 Validator vScript: ZTP upload chassis numbers: /usr/bin/vconfd_script_upload_chassis_number_file.sh -cli path /home/admin/chassis_numbers_safe.csv

Note: The above are legitimate commands, and the logs will not distinguish between legitimate and malicious use. Organisations that observe these logs and are uncertain about their origin or intent should contact the Cisco Technical Assistance Center (TAC) for further assistance.

Description	**Indicator**
IP address connecting as rogue device and exploiting CVE-2026-20245	126.51.108[.]152
IP address connecting as rogue device	76.92.245[.]217
IP address connecting as rogue device	207.190.37[.]94
IP address connecting as rogue device	23.245.7[.]178
IP address connecting as rogue device	153.186.231[.]233
IP address connecting as rogue device	167.179.79[.]189
IP address connecting as rogue device	45.32.38[.]160
IP address connecting as rogue device	209.137.225[.]101

Filename	**Description**	**SHA256**
/home/admin/.orig_vbond_vsmart_tenant_list	Backup configuration file	Not recovered
/home/admin/.orig_vbond_vsmart_tenant_list.state	State file	Not recovered
/home/admin/.orig_passwd	Backup password file	Not recovered
/home/admin/.orig_shadow	Backup password file	Not recovered
/home/admin/evil_tenant.csv	Remnant of malicious CSV file exploiting CVE-2026-20245	b82936f37648518425c7d3cf9e09eaffa41d7cdb3840f6a40287e3a108880f7b

Reference:

1. Zero-Day Exploitation of Vulnerability (CVE-2026-20245) in Cisco Catalyst SD-WAN Manager | Google Cloud Blog
2. Cisco Catalyst SD-WAN Controller, Catalyst SD-WAN Manager, and Catalyst SD-WAN Validator Authenticated Privilege Escalation Vulnerability
3. CVE-2026-20127 - Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
4. CVE-2026-20182 - Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
5. Cisco Catalyst SD-WAN Hardening Guide