INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-25 13:59 UTC

Cisco Catalyst SD-WAN Zero-Day CVE-2026-20245 Actively Exploited for Root Access and Management Plane Compromise

CVE VULNERABILITY | **CRITICAL** | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0350
Type	CVE Vulnerability
CVE ID	CVE-2026-20245
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.0992 (95th percentile)
Affected Products	Cisco Catalyst SD-WAN Manager (specific versions unverified from available source data)
Published	8 hours ago
Discovery Source	Serper

Executive Summary

A critical zero-day vulnerability in Cisco Catalyst SD-WAN Manager is reported to allow unauthenticated or low-privilege attackers to gain root-level access and fully compromise the network management plane. Organizations running Cisco Catalyst SD-WAN Manager are at risk of complete loss of WAN visibility and control, with secondary risk of lateral movement into connected enterprise networks. Active exploitation is reported across secondary sources; no official Cisco patch or advisory has been publicly confirmed at this time, requiring immediate compensating controls pending official confirmation.

Technical Analysis

CVE-2026-20245 is a reported critical zero-day in Cisco Catalyst SD-WAN Manager based on secondary source reporting (Cloud Security Alliance labs, SOC Prime, The Register dated 2026-06-24). Secondary sources describe the vulnerability as enabling unauthenticated or low-privilege remote privilege escalation to root with command execution capability on the management plane. CWE mapping: CWE-78 (OS Command Injection) and CWE-269 (Improper Privilege Management). MITRE ATT&CK techniques: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1059 (Command and Scripting Interpreter), T1078 (Valid Accounts). CVSS base score is reported at 9.8 (Critical); EPSS score 0.099 places this in the 95th percentile for exploitation probability. Affected versions are unverified in available secondary

source data. No NVD record or official Cisco PSIRT advisory has been independently confirmed from authoritative sources as of this publication. CISA KEV inclusion is not confirmed. Patch status: unknown pending official Cisco advisory. All technical specifics are sourced exclusively from T3 secondary references; treat version scope and exploitation mechanics as provisional until Cisco PSIRT publishes.

Action Checklist

1. Step 1: Containment, Immediately restrict network access to Cisco Catalyst SD-WAN Manager interfaces. Block inbound connections to the management plane from untrusted networks at the perimeter firewall. Disable external-facing SD-WAN Manager access where operationally feasible until a Cisco PSIRT advisory and patch are available. Reference NIST AC-17 (Remote Access) for authorization controls on remote management interfaces.
2. Step 2: Detection, Query authentication and privilege logs on SD-WAN Manager nodes for anomalous root-level command execution, unexpected account privilege changes, and unauthenticated or failed-then-succeeded login sequences. Review system init configurations for unauthorized modifications (D3-SICA). Audit local accounts for new or altered entries (D3-LAM). Monitor for T1190 indicators: unusual inbound HTTP/API requests to management endpoints, especially those triggering process spawning. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence. Reference CIS 8.2 (Collect Audit Logs) to confirm logging is enabled on all SD-WAN Manager nodes.
3. Step 3: Eradication, Monitor Cisco Security Advisory feed (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory) for the official patch release for CVE-2026-20245. As of this publication, no Cisco PSIRT advisory has been confirmed; apply the fix immediately upon availability. Until patched: enforce least-privilege access on all SD-WAN Manager accounts, disable unused management interfaces, and rotate all credentials associated with the management plane (D3-CRO). Reference NIST AC-6 (Least Privilege) and CIS 7.3 (Perform Automated Operating System Patch Management).
4. Step 4: Recovery, After patching, validate that no unauthorized accounts or scheduled tasks persist on SD-WAN Manager nodes. Perform system file integrity checks for unauthorized modifications (D3-SFA). Confirm management plane telemetry and SD-WAN policy configurations match pre-incident baselines. Re-enable remote management access only after MFA enforcement is confirmed on all management accounts (D3-MFA, CIS 6.5). Reference NIST AU-9 (Protection of Audit Information) to verify audit log integrity post-incident.
5. Step 5: Post-Incident, Review whether management interfaces were unnecessarily internet-exposed, violating NIST AC-17 and CIS 4.4 (Implement and Manage a Firewall on Servers). Evaluate separation of duties for SD-WAN management roles per NIST AC-5. Assess whether privileged access to the management plane requires a dedicated administrator account model per CIS 5.4. Document the gap between zero-day disclosure and patch availability and update the organizational vulnerability management SLA per CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and executive stakeholders if forensic analysis confirms unauthorized root-level access to the SD-WAN Manager was achieved, if SD-WAN policy configurations show unauthorized modification (indicating attacker-controlled routing or traffic steering), if any connected enterprise network segments accessible via the management plane show indicators of lateral movement, or if the organization is subject to regulatory frameworks (e.g., HIPAA, PCI-DSS, NERC CIP) requiring breach notification — given CVE-2026-20245's CVSS 9.8 rating and active exploitation status with no confirmed official patch, the blast radius justifies immediate escalation without waiting for forensic confirmation.
Recovery Notes	After patching and re-hardening, maintain enhanced monitoring on SD-WAN Manager authentication and API activity for a minimum of 30 days, specifically watching for re-exploitation attempts against the same attack surface and any signs of attacker re-entry via persistence mechanisms that may have survived eradication. Validate SD-WAN policy configuration integrity against the pre-incident baseline on a daily basis for the first two weeks post-recovery, as attackers who achieved management plane access may have staged delayed configuration changes. Because no official Cisco PSIRT advisory has been confirmed at time of this analysis, continue monitoring the Cisco Security Advisory feed daily and treat any Cisco-published workaround guidance as superseding the interim compensating controls documented here.
Forensic Artifacts	SD-WAN Manager application authentication logs (/var/log/nms/vmanage-aaa.log) — will contain the exploit's authentication bypass or privilege escalation sequence specific to CVE-2026-20245, including the source IP of the attacker and the exact API endpoint targeted | vManage REST API access logs (/var/log/nms/vmanage-server.log) — HTTP request records showing anomalous POST/GET calls to /dataservice/ management endpoints, particularly unauthenticated requests that received successful (HTTP 200) responses, which would be the direct signature of this unauthenticated-access vulnerability | Linux OS audit log syscall records (/var/log/audit/audit.log) — SYSCALL execve events showing root-owned process execution spawned from the vmanage service account, specifically shell interpreter invocations (bash, sh, python) that indicate post-exploitation command execution following root privilege acquisition | SD-WAN Manager local account and sudoers state (/etc/passwd, /etc/shadow, /etc/sudoers, /etc/sudoers.d/) — file modification timestamps and content changes revealing attacker-created local OS accounts or sudo privilege grants used to maintain root-level persistence after initial exploitation of CVE-2026-20245 | vManage SD-WAN policy configuration export (via /dataservice/template/policy/vsmart and /dataservice/template/feature) — JSON diff against pre-incident baseline revealing whether the attacker leveraged management plane root access to modify WAN routing policy, traffic steering rules, or security zone configurations, indicating secondary network impact beyond the manager node itself

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to Cisco Catalyst SD-WAN Manager interfaces. Block inbound connections to the management plane from untrusted networks at the perimeter firewall. Disable external-facing SD-WAN Manager access where operationally feasible until a Cisco PSIRT advisory and patch are available. Reference NIST AC-17 (Remote Access) for authorization controls on remote management interfaces.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Use iptables or Windows Firewall to immediately block inbound TCP 443, 8443, and any custom SD-WAN Manager management ports from non-administrative source CIDRs. On the upstream perimeter router or firewall, add an explicit deny ACL for the SD-WAN Manager management IP(s). For teams without a centralized firewall console, run: 'iptables -I INPUT -p tcp --dport 443 -s 0.0.0.0/0 -j DROP' followed by a permit rule for the specific admin jump-host IP. Document the ACL change with timestamp for chain-of-custody.

Evidence: Before isolating or restricting access, capture: (1) full netstat output showing all active TCP sessions to SD-WAN Manager management ports ('netstat -antp' on Linux or 'Get-NetTCPConnection' on Windows); (2) currently authenticated session tokens and active API sessions from SD-WAN Manager's session database or logs (typically under /var/log/nms/ or equivalent); (3) running process list ('ps auxf' or equivalent) to identify any anomalous child processes spawned by the SD-WAN Manager service prior to network isolation. These are volatile and will not survive session termination or service restart.

Step 2: Detection — Query authentication and privilege logs on SD-WAN Manager nodes for anomalous root-level command execution, unexpected account privilege changes, and unauthenticated or failed-then-succeeded login sequences. Review system init configurations for unauthorized modifications (D3-SICA). Audit local accounts for new or altered entries (D3-LAM). Monitor for T1190 indicators: unusual inbound HTTP/API requests to management endpoints, especially those triggering process spawning. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence. Reference CIS 8.2 (Collect Audit Logs) to confirm logging is enabled on all SD-WAN Manager nodes.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: On the SD-WAN Manager host (Linux-based), run: 'grep -E "(sudo|su |root|FAILED|Accepted)" /var/log/auth.log | sort -k1,2' to surface privilege escalation and authentication anomalies. Parse SD-WAN Manager application logs (typically /var/log/nms/vmanage-server.log) for HTTP POST requests to /dataservice/ or /j_security_check endpoints with unexpected source IPs or unusual response codes (200 following prior 401/403 sequences). Check /etc/passwd and /etc/shadow modification timestamps: 'stat /etc/passwd /etc/shadow'. Use 'ausearch -m USER_AUTH,USER_ROLE_CHANGE,SYSCALL -ts today' if auditd is running to identify privilege-related syscalls. For network-side detection without a SIEM, run Wireshark or tcpdump on the management interface: 'tcpdump -i eth0 -w sdwan_mgmt_capture.pcap port 443 or port 8443' and inspect for anomalous API call patterns.

Evidence: Capture before any account remediation or service restart: (1) /var/log/nms/vmanage-server.log and vmanage-aaa.log covering the window from 72 hours prior to detection — these will contain unauthenticated API request patterns specific to CVE-2026-20245 exploitation; (2) /etc/passwd, /etc/shadow, and /etc/sudoers — modification timestamps and hashes (sha256sum) to detect post-exploitation account creation; (3) auditd logs (/var/log/audit/audit.log) filtered for SYSCALL execve events showing root-owned processes spawned from the vmanage service user; (4) active session list from SD-WAN Manager CLI ('show users' or equivalent vManage API endpoint /dataservice/admin/user) capturing any unauthorized local accounts added by the attacker; (5) memory image of the vmanage-server process if exploitation is suspected active, using dd or LiME kernel module before any service restart.

Step 3: Eradication — Monitor Cisco Security Advisory feed (https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory) for the official patch release. Apply the Cisco-published fix immediately upon availability. Until patched: enforce least-privilege access on all SD-WAN Manager accounts, disable unused management interfaces, and rotate all credentials associated with the management plane (D3-CRO). Reference NIST AC-6 (Least Privilege) and CIS 7.3 (Perform Automated Operating System Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Prior to patch availability, on SD-WAN Manager: (1) enumerate all local OS accounts and vManage application accounts — remove any not present in your pre-incident account inventory baseline; use 'awk -F: "$3 >= 1000" /etc/passwd' to list non-system accounts and cross-reference against the authorized account list; (2) lock the vmanage application service account from OS-level shell access: 'usermod -s /sbin/nologin vmanage'; (3) rotate all SD-WAN Manager admin credentials via the vManage UI (/administration/users) and immediately revoke any API tokens or OAuth credentials associated with the management plane; (4) disable the vManage REST API if not operationally required: stop the API service or apply an ACL restricting API access to the admin jump-host IP exclusively. Use 'crontab -l' and 'systemctl list-timers' to check for persistence mechanisms installed by the attacker before applying the patch.

Evidence: Before patching or reimaging, preserve: (1) full filesystem snapshot or dd image of the SD-WAN Manager VM disk — the CVE-2026-20245 exploit likely wrote a webshell, modified a startup script, or created a privileged cron entry that will be destroyed by reimaging; (2) 'crontab -l -u root' and contents of /etc/cron.d/, /etc/cron.daily/, /etc/rc.local — attacker persistence for root-level access on network management appliances commonly targets init and scheduled task locations; (3) list of all installed packages and recent package modifications: 'rpm -qa --last | head -50' or 'dpkg -l' with timestamps, to identify attacker-installed tooling; (4) network connections active at time of eradication: 'ss -tulnp' capturing any backdoor listener ports opened post-exploitation. Note: patch application constitutes an eradication action that alters system state — all volatile and semi-volatile evidence listed above must be captured before the patch is applied.

Step 4: Recovery — After patching, validate that no unauthorized accounts or scheduled tasks persist on SD-WAN Manager nodes. Perform system file integrity checks for unauthorized modifications (D3-SFA). Confirm management plane telemetry and SD-WAN policy configurations match pre-incident baselines. Re-enable remote management access only after MFA enforcement is confirmed on all management accounts (D3-MFA, CIS 6.5). Reference NIST AU-9 (Protection of Audit Information) to verify audit log integrity post-incident.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AC-17 (Remote Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Run a file integrity check against known-good SD-WAN Manager binary and configuration hashes using sha256sum on critical paths: /opt/cisco/vmanage/, /etc/viptela/, and web application directories. Compare against Cisco-published checksums from the patched release advisory. Use AIDE (Advanced Intrusion Detection Environment) if pre-incident baseline was established: 'aide --check'. For SD-WAN policy configuration drift, export the current running policy via the vManage API (/dataservice/template/policy/vsmart) and diff against a pre-incident JSON export stored in version control. Re-enable management access only from the hardened jump-host with MFA enforced — validate MFA is active by attempting login without the second factor and confirming rejection. Confirm audit logging resumed and is forwarding to an off-host syslog receiver.

Evidence: At recovery stage, evidence focus shifts to integrity validation rather than volatile capture. Document: (1) output of the file integrity check with hashes and timestamps as the authoritative record that eradication was complete; (2) before re-enabling remote access, capture a final 'show users' / account audit confirming no residual unauthorized accounts — this is your post-eradication clean-state attestation; (3) SD-WAN policy configuration export (JSON) post-patch as the restored-baseline record; (4) audit log continuity check — confirm no gaps in AU log timestamps between the incident window and recovery, as log gaps may indicate attacker tampering with AU-9-protected records (check /var/log/nms/ log rotation and remote syslog receipt timestamps). Retain all evidence captured across all prior phases for a minimum of 90 days or per organizational retention policy, whichever is longer.

Step 5: Post-Incident — Review whether management interfaces were unnecessarily internet-exposed, violating NIST AC-17 and CIS 4.4 (Implement and Manage a Firewall on Servers). Evaluate separation of duties

for SD-WAN management roles per NIST AC-5. Assess whether privileged access to the management plane requires a dedicated administrator account model per CIS 5.4. Document the gap between zero-day disclosure and patch availability and update the organizational vulnerability management SLA per CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (Lessons Learned)

Controls: NIST AC-17 (Remote Access), NIST AC-5 (Separation Of Duties), NIST AU-11 (Audit Record Retention), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For a 2-person team conducting post-incident review without a GRC platform: create a structured lessons-learned document capturing (1) the timeline from first external disclosure of CVE-2026-20245 to detection on your environment — this delta is your effective exposure window and should drive the vulnerability SLA update; (2) a network diagram annotation showing which SD-WAN Manager interfaces were reachable from untrusted networks and why — use 'nmap -sV -p 443,8443,830 ' from an external vantage to simulate attacker reachability; (3) a role audit table for all vManage application roles, comparing current role assignments against the principle of least-privilege and separation of duties — specifically whether the same account had both policy-push and user-administration privileges, which would have amplified post-exploitation blast radius for CVE-2026-20245's management plane compromise.

Evidence: Post-incident evidence to retain and reference in the lessons-learned report: (1) the complete incident timeline log with timestamps from all phases — this is the primary artifact for regulatory notification assessment if the SD-WAN Manager had visibility into PII-handling network segments; (2) the pre- and post-incident account inventory comparison showing any accounts created during the compromise window; (3) the network exposure assessment output (nmap or firewall rule export) documenting the attack surface that enabled exploitation of CVE-2026-20245; (4) the patch lag timeline — date of zero-day secondary source disclosure versus date of Cisco PSIRT official advisory versus date of patch application — as a measured input to updating the vulnerability management SLA under CIS 7.1.

Detection Guidance

Priority detection actions while no official Cisco advisory is available: (1) Enable and centralize syslog and audit logging from all Cisco Catalyst SD-WAN Manager nodes if not already active (CIS 8.2, NIST AU-2, AU-12). (2) Search logs for root-level process execution originating from web or API service processes, which would indicate CWE-78 OS command injection exploitation. (3) Identify any privilege escalation events (UID changes to 0/root) in system logs, correlating with T1068 and T1190 activity patterns. (4) Monitor for unexpected new local accounts or modifications to existing account privilege levels on SD-WAN Manager nodes (D3-LAM). (5) Alert on inbound connections to SD-WAN Manager management ports from external or unexpected IP ranges. (6) Analyze system initialization and configuration files for unauthorized changes consistent with persistence (D3-SICA). No confirmed IOC signatures are available from authoritative sources at this time; detection must rely on behavioral and anomaly-based methods until Cisco publishes indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs available from authoritative sources`	CVE-2026-20245 IOCs have not been published by Cisco PSIRT or CISA as of source data used. Monitor Cisco Security Advisory feed and CISA KEV for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation
- **T1059** — Command and Scripting Interpreter
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://www.rescana.com/post/cisco-catalyst-sd-wan-zero-day-cve-202...	T3
Cisco SD-WAN Zero-Day: Unpatched Root Privilege Escalation	https://labs.cloudsecurityalliance.org/research/csa-research-note-c...	T3
CVE-2026-20245: Cisco SD-WAN Manager Zero-Day - SOC Prime	https://socprime.com/blog/cve-2026-20245-analysis/	T3
The hits keep on coming for Cisco vulnerabilities - The Register	https://www.theregister.com/security/2026/06/24/the-hits-keep-on-co...	T3
Cisco SD-WAN Manager Zero-Day Enables Root Command Execution	https://www.reddit.com/r/SecOpsDaily/comments/1txpa58/cve202620245_...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20245	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-06-25 13:59 UTC by TJS Security Command Center