INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 18:51 UTC

Second CVSS 10.0 Cisco SD-WAN Exploit This Year Signals Sustained Campaign Against Network Control Planes

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0182
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cisco Catalyst SD-WAN Controller (specific versions unconfirmed from available sources)
Published	2026-05-14T16:25:31
Discovery Source	Rss

Executive Summary

A maximum-severity authentication bypass vulnerability in Cisco Catalyst SD-WAN controllers is under active exploitation, with CISA issuing an Emergency Directive requiring immediate remediation. Unauthenticated remote attackers can gain full administrative control over SD-WAN infrastructure, enabling traffic manipulation and lateral movement across distributed WAN environments. Organizations running Cisco SD-WAN face risk of complete network control plane compromise, which can disrupt operations across all sites connected through that infrastructure.

Technical Analysis

The vulnerability affects Cisco Catalyst SD-WAN Controller and involves chained weaknesses: CWE-306 (missing authentication for critical function) and CWE-287 (improper authentication), which together enable unauthenticated access to administrative interfaces. CWE-78 (OS command injection) enables post-authentication code execution, allowing an attacker who bypasses authentication to execute arbitrary OS commands. CVSS base score is 9.5 per Cisco Security Advisory cisco-sa-sdwan-rpa-EHchtZk; CVSS vector to be updated when NVD publishes official score. MITRE ATT&CK techniques mapped include T1190 (exploit public-facing application), T1078 (valid accounts), T1133 (external remote services), T1021 (remote services), T1557 (adversary-in-the-middle), and T1565/T1565.002 (data manipulation). Affected versions and patch availability are specified in Cisco Security Advisory cisco-sa-sdwan-rpa-EHchtZk, consult that advisory directly before remediation. Active exploitation is confirmed; CISA has issued an Emergency Directive. No confirmed IOCs or attributed threat actor at time of publication.

Action Checklist

1. Step 1: Containment, Immediately restrict administrative access to Cisco Catalyst SD-WAN controllers to trusted management networks only. Block direct internet exposure of controller management interfaces at the perimeter. Verify no management plane interfaces are internet-accessible. Consult Cisco advisory cisco-sa-sdwan-rpa-EHchtZk for specific interface and service recommendations.
2. Step 2: Detection, Review controller authentication logs for anomalous unauthenticated access attempts or unexpected administrative sessions. Look for command execution events, configuration changes, or new administrative accounts created outside your change management process. Correlate against T1190 and T1078 indicators in your SIEM. Check for unexpected BGP route changes or traffic policy modifications that could indicate T1565.002 (transmit data manipulation).
3. Step 3: Eradication, Apply the patch or workaround specified in Cisco Security Advisory cisco-sa-sdwan-rpa-EHchtZk as soon as it is available. If a patch is not yet available, implement compensating controls per the advisory's workaround guidance, including restricting access to the vManage and controller interfaces. Rotate all administrative credentials for SD-WAN controllers regardless of whether compromise is confirmed.
4. Step 4: Recovery, After patching, audit all SD-WAN configuration objects, routing policies, and administrative accounts for unauthorized changes. Validate traffic policy integrity across all WAN edges. Confirm no persistence mechanisms were introduced (new admin accounts, API tokens, or modified device templates). Monitor controller logs for at least 30 days post-remediation, or per your incident response policy, for signs of re-exploitation.
5. Step 5: Post-Incident, Conduct a review of your management plane exposure across all Cisco infrastructure, not just SD-WAN. Assess whether out-of-band management, zero-trust access to network controllers, and automated patch SLAs for critical network infrastructure are in place. Map gaps to NIST CSF PR.AC and PR.PT controls.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and senior leadership immediately if any of the following are confirmed: unauthorized administrative accounts discovered in vManage, evidence of routing policy modification or BGP manipulation affecting production traffic, SD-WAN controller management interface was internet-accessible for any period after the CISA Emergency Directive publication date, or if the organization is subject to NERC CIP, HIPAA, or FedRAMP compliance frameworks where network control plane compromise triggers mandatory breach notification assessment.

Recovery Notes	Post-patch, perform a complete audit of all vManage configuration objects — device templates, routing policies, and security policies — against your last change-controlled baseline before declaring recovery complete, as an attacker with full administrative access could have pre-positioned persistent configuration changes designed to survive a simple patch cycle. Monitor vManage audit logs and SD-WAN edge 'show sdwan control connections' output daily for the first two weeks and weekly for 30 days total, specifically watching for re-authentication attempts from previously blocked source IPs or unexpected vSmart controller re-registrations that could indicate a second-stage implant. Do not restore any management plane access from the internet until out-of-band management or a zero-trust network access (ZTNA) solution is validated and operational.
Forensic Artifacts	vManage Audit Log (Administration > Audit Log or GET /dataservice/auditlog): primary forensic source for this exploit — an authentication bypass will produce HTTP 200 success responses to /j_security_check or /dataservice/client/token without valid credential submission; look for session creation events from non-management source IPs with no corresponding MFA or RADIUS authentication record in the upstream identity provider. | vManage NMS Web Server Access Logs (/var/log/nms/ on the vManage appliance): will contain raw HTTP request records showing the specific URI paths and source IPs used in the authentication bypass exploitation attempt, including any subsequent API calls made by the attacker to enumerate users (GET /dataservice/admin/user), download configurations (GET /dataservice/template/device), or push policy changes (POST /dataservice/template/policy/activate). | SD-WAN Edge Router Policy and Routing State ('show sdwan policy from-vsmart' and 'show ip route vrf all'): if the attacker used vManage administrative access to push malicious traffic policies or routing changes (T1565.002), the edge routers will retain the injected policy objects even if the vManage audit log has been tampered with — this provides an independent forensic record of configuration manipulation. | vManage Configuration Database Backup ('request nms configuration-db backup'): a snapshot of the vManage database at time of suspected compromise preserves the full state of device templates, policy objects, and administrative accounts that an attacker with full admin access could have modified, enabling forensic comparison against pre-incident backups to enumerate every unauthorized change. | Network Flow Records (NetFlow/IPFIX) from WAN Edge Routers: capture traffic flows from vManage management interfaces for the 72-hour window prior to containment — an attacker who gained administrative control and began traffic manipulation (T1565.002) or used the SD-WAN fabric for lateral movement (T1599 — Network Boundary Bridging) will leave anomalous flow patterns showing unexpected inter-VRF traffic or management plane traffic to non-standard destinations.

Per-Action IR Details

Step 1: Containment — Immediately restrict administrative access to Cisco Catalyst SD-WAN controllers to trusted management networks only. Block direct internet exposure of controller management interfaces at the perimeter. Verify no management plane interfaces are internet-accessible. Consult Cisco advisory cisco-sa-sdwan-rpa-EHchtZk for specific interface and service recommendations.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further unauthorized access while preserving forensic state; CSF [RS] function — execute IR plan and mitigate active threat.

Controls: NIST IR-4 (Incident Handling) — implement containment as part of the incident handling capability, NIST SC-7 (Boundary Protection) — restrict management plane traffic to trusted network segments only, NIST AC-17 (Remote Access) — enforce access restrictions on remote administrative interfaces, CIS 4.4 (Implement and Manage a Firewall on Servers) — apply ACLs blocking internet-facing exposure of vManage and controller management ports, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure) — validate and enforce

hardened network device configuration blocking unauthenticated external access

Compensating: Without a NGFW or NAC solution: immediately apply ACLs on the upstream router or L3 switch feeding the SD-WAN controller management interface to permit only your dedicated management VLAN source IPs. Use 'show ip access-lists' and 'show run interface' on the upstream device to confirm ACL application. If the vManage instance is cloud-hosted (AWS/Azure), modify the Security Group or NSG to remove port 443 and 8443 inbound from 0.0.0.0/0 immediately. Run a quick external validation using nmap: 'nmap -p 443,8443,22,830 ' from an external host to confirm interfaces are no longer reachable.

Evidence: Before restricting access, capture: (1) 'show running-config' full output from vManage and all SD-WAN controllers to document current state and detect any unauthorized configuration injections; (2) current active sessions via 'show users' or vManage REST API GET /dataservice/admin/user/sessions to enumerate unexpected administrative sessions; (3) netstat or equivalent on the vManage host to document all listening ports and active TCP connections pre-containment; (4) vManage audit log export (Administration > Audit Log in vManage GUI, or GET /dataservice/auditlog) covering the prior 72 hours for authentication events and configuration change records before any ACL disrupts attacker connectivity.

Step 2: Detection — Review controller authentication logs for anomalous unauthenticated access attempts or unexpected administrative sessions. Look for command execution events, configuration changes, or new administrative accounts created outside your change management process. Correlate against T1190 and T1078 indicators in your SIEM. Check for unexpected BGP route changes or traffic policy modifications that could indicate T1565.002 (transmit data manipulation).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: analyze log data to determine scope, attack vector, and indicators of compromise; CSF [DE] function — monitor and analyze adverse events to confirm incident.

Controls: NIST SI-4 (System Monitoring) — monitor SD-WAN controller management plane for anomalous authentication and configuration change activity, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review vManage audit logs and controller authentication records for T1190/T1078 indicators, NIST AU-2 (Event Logging) — ensure authentication events, session creation, and configuration changes are captured in vManage audit log, NIST IR-5 (Incident Monitoring) — track and document indicators discovered during SD-WAN controller log analysis, CIS 8.2 (Collect Audit Logs) — ensure vManage audit logging is enabled and logs are forwarded off-controller before potential tampering

Compensating: Without a SIEM: export vManage audit logs directly via REST API: 'curl -k -X GET https:///dataservice/auditlog -H "Cookie: " > auditlog.json' and parse with jq for entries where 'logActivity' contains 'login', 'addUser', 'editPolicy', or 'deletePolicy' with unexpected usernames or source IPs. For BGP route deviation detection without a NMS, run 'show bgp summary' and 'show ip route' snapshots from SD-WAN edge routers at 15-minute intervals using a simple bash cron script and diff the output. Deploy the free Cisco-published Sigma rule equivalent by manually grepping vManage auth logs for HTTP 200 responses to POST /j_security_check or /dataservice/client/token from source IPs outside your management subnet.

Evidence: Collect before or concurrent with analysis: (1) vManage audit log entries (GET /dataservice/auditlog) filtering for 'logActivity' values of 'Login', 'Create User', 'Edit User', 'Edit Policy', and 'Activate Policy' — an auth bypass exploit would produce successful login records with no preceding valid credential submission; (2) vManage NMS database query for admin account table (if accessible) to identify accounts with creation timestamps outside change windows — MITRE T1136 (Create Account) is a common post-exploitation step after T1190; (3) SD-WAN edge router 'show sdwan policy from-vsmart' output to detect unauthorized traffic policy pushes from a potentially compromised vManage; (4) BGP routing table snapshots ('show bgp vpnv4 unicast all') from all WAN edges before and after the suspected exploitation window to detect T1565.002 route manipulation; (5) Web server access logs from vManage (typically at /var/log/nms/ on the vManage appliance) for anomalous HTTP POST requests to authentication endpoints from non-management source IPs.

Step 3: Eradication — Apply the patch or workaround specified in Cisco Security Advisory cisco-sa-sdwan-rpa-EHchtZk as soon as it is available. If a patch is not yet available, implement compensating controls per the advisory's workaround guidance, including restricting access to the vManage and controller interfaces. Rotate all administrative credentials for SD-WAN controllers regardless of whether compromise is

confirmed.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability and any artifacts of compromise from the environment; CSF [RS] function — verify threat removal and validate eradication effectiveness.

Controls: NIST SI-2 (Flaw Remediation) — apply Cisco-issued patch for the SD-WAN authentication bypass vulnerability per cisco-sa-sdwan-rpa-EHchtZk advisory guidance, NIST IR-4 (Incident Handling) — execute eradication phase of incident handling plan including credential rotation and account audit, NIST IA-5 (Authenticator Management) — rotate all SD-WAN controller administrative credentials and revoke any API tokens issued prior to containment, CIS 7.3 (Perform Automated Operating System Patch Management) — apply Cisco SD-WAN software update from Cisco Software Center to affected controller versions, CIS 7.4 (Perform Automated Application Patch Management) — validate patch version across all vManage, vSmart, and vBond controller nodes in the SD-WAN fabric, CIS 5.2 (Use Unique Passwords) — enforce unique, rotated credentials for all vManage administrative accounts post-eradication

Compensating: If the Cisco patch is not yet available: implement the workaround from cisco-sa-sdwan-rpa-EHchtZk (typically restricting the vulnerable service or interface binding as directed by Cisco PSIRT). For credential rotation without an enterprise PAM tool, use vManage CLI: 'request nms certificate invalidate' to revoke existing sessions, then manually reset each admin account password via 'vshell' administrative interface or GUI Administration > Manage Users. Document each rotation with timestamp and operator name. Generate new API tokens only from a hardened management workstation. Set a calendar reminder to re-evaluate patch availability from Cisco's PSIRT feed every 24 hours until the fix is applied.

Evidence: Before patching, preserve: (1) full 'show version' output from vManage, vSmart, and vBond to document pre-patch software versions for chain-of-custody records; (2) export of all current administrative user accounts and their last-login timestamps via vManage REST API GET /dataservice/admin/user before rotation — preserve this to compare against post-incident account audit; (3) copy of any newly discovered admin accounts or API tokens that were not in your authorized account inventory, as these are likely attacker-created persistence mechanisms (T1136/T1098) and constitute forensic evidence; (4) snapshot of the vManage configuration database (use 'request nms configuration-db backup' CLI command) to preserve the potentially tampered configuration state before eradication overwrites it.

Step 4: Recovery — After patching, audit all SD-WAN configuration objects, routing policies, and administrative accounts for unauthorized changes. Validate traffic policy integrity across all WAN edges. Confirm no persistence mechanisms were introduced (new admin accounts, API tokens, or modified device templates). Monitor controller logs for at least 30 days post-remediation for signs of re-exploitation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation, verify integrity, and implement enhanced monitoring; CSF [RC] function — execute recovery plan and confirm operational integrity.

Controls: NIST IR-4 (Incident Handling) — execute recovery phase including system integrity validation and enhanced monitoring period, NIST CM-3 (Configuration Change Control) — compare current SD-WAN configuration state against last known-good baseline to identify unauthorized modifications, NIST SI-7 (Software, Firmware, and Information Integrity) — employ integrity verification to detect unauthorized changes to SD-WAN device templates, routing policies, and controller configurations, NIST AU-11 (Audit Record Retention) — retain SD-WAN controller audit logs for the 30-day post-remediation monitoring period to support re-exploitation detection, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — audit all vManage administrative accounts against authorized inventory and remove unauthorized entries, CIS 4.6 (Securely Manage Enterprise Assets and Software) — validate SD-WAN configuration integrity against version-controlled baselines

Compensating: Without a dedicated configuration management tool: export the full current SD-WAN configuration via 'show running-config' (or vManage REST API GET /dataservice/template/device) and perform a manual diff against your last change-controlled backup using 'diff -u baseline-config.txt current-config.txt'. For API token audit, query GET /dataservice/admin/apitoken to enumerate all active tokens and compare against your authorized token registry — revoke any unrecognized entries immediately. For the 30-day monitoring window without a SIEM, configure vManage email alerts (Administration > Email Notifications) for login events and policy change events, forwarding to a dedicated security mailbox reviewed daily. Use osquery with a query against the process table on the vManage Linux host to

detect unexpected processes: 'SELECT name, path, cmdline, pid FROM processes WHERE name NOT IN (expected_process_list)'.

Evidence: During recovery validation, document: (1) diff output comparing pre-incident configuration snapshot (captured in Step 3 evidence) against post-patch configuration to identify any unauthorized policy objects, route-maps, or device templates that survived eradication; (2) complete account audit report listing all vManage users, their roles, creation dates, and last login — compare against pre-incident baseline to confirm no attacker-created accounts persist; (3) 'show sdwan control connections' output from all WAN edges confirming they connect only to authorized vSmart controllers — a compromised vManage could have pushed unauthorized vSmart controller addresses to edges; (4) BGP routing table comparison across all WAN edges confirming routing state matches pre-incident baseline, specifically checking for any route leaks or unauthorized redistribution policies introduced via T1565.002.

Step 5: Post-Incident — This is the second CVSS 10.0-class Cisco network management vulnerability targeted in 2026. Conduct a review of your management plane exposure across all Cisco infrastructure, not just SD-WAN. Assess whether out-of-band management, zero-trust access to network controllers, and automated patch SLAs for critical network infrastructure are in place. Map gaps to NIST CSF PR.AC and PR.PT controls.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update policies and detection capabilities, and improve organizational posture against recurrence; CSF [GV, ID] functions — update governance and improve identification capabilities.

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to incorporate SD-WAN management plane compromise scenarios, NIST IR-8 (Incident Response Plan) — revise IR plan to include network control plane compromise as a specific incident category with defined response procedures, NIST RA-3 (Risk Assessment) — formally assess management plane exposure risk across all Cisco infrastructure following the second CVSS 10.0-class exploitation in 2026, NIST CM-7 (Least Functionality) — review and restrict services, protocols, and interfaces exposed on all Cisco network management platforms, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish a formal process to receive and act on Cisco PSIRT advisories within defined SLAs for critical-severity findings, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update vulnerability management process to include critical network infrastructure (SD-WAN, DNA Center, ISE) with accelerated patch SLAs matching CISA KEV timelines, CIS 7.2 (Establish and Maintain a Remediation Process) — document risk-based remediation SLAs specifically for CVSS 9.0+ vulnerabilities in network control plane components

Compensating: Without a formal vulnerability management platform: create a network management plane inventory spreadsheet (hostnames, management IPs, software versions, internet exposure Y/N) and review it against the Cisco PSIRT advisory feed (https://tools.cisco.com/security/center/publicationListing) on a weekly basis — assign this as a named responsibility, not a shared task. For out-of-band management without a dedicated OOB network: configure a dedicated management VLAN with no routing to the production network, accessible only via a jump host requiring MFA (deploy Teleport or Apache Guacamole as a free OOB-adjacent solution). Draft a one-page patch SLA policy that classifies CVSS 9.0+ actively exploited vulnerabilities in network management platforms as 24-72 hour mandatory remediation, requiring VP-level exception approval to defer.

Evidence: For lessons-learned documentation: (1) compile a timeline of the incident from initial advisory publication to full remediation, noting any gaps between CISA Emergency Directive issuance and your containment action — this delta is a key metric for process improvement; (2) inventory of all Cisco management plane components (vManage, DNA Center, Cisco ISE, Prime Infrastructure, APIC) with their current software versions and internet exposure status — produced as an artifact of the post-incident management plane review; (3) comparison of this incident's response timeline against the first CVSS 10.0-class Cisco management plane vulnerability in 2026, identifying whether detection and containment improved — recurring targeting of Cisco control planes by the same campaign suggests a persistent threat actor and warrants formal threat actor profiling against MITRE ATT&CK Groups.

Detection Guidance

Query authentication logs on vManage and SD-WAN controllers for sessions that succeeded without valid credential presentation, particularly originating from external IPs. Look for: (1) Admin account creation or privilege escalation outside change windows. (2) Configuration template modifications not tied to approved change requests. (3) Unexpected CLI command execution events in controller audit logs, which may indicate CWE-78 exploitation. (4) Anomalous routing policy changes or traffic steering modifications across WAN edges (T1565.002). (5) New API tokens or service account activity. SIEM detection should correlate T1190 (external exploit attempts against the controller management interface) with T1078 (subsequent use of valid-looking sessions). No public IOCs (IPs, hashes, domains) are confirmed in available sources at time of writing.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1133** — External Remote Services
- **T1565.002** — Transmitted Data Manipulation
- **T1557** — Adversary-in-the-Middle
- **T1565** — Data Manipulation
- **T1021** — Remote Services
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

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
T1078	Valid Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1565.002	Transmitted Data Manipulation	Impact
T1557	Adversary-in-the-Middle	Credential-Access
T1565	Data Manipulation	Impact
T1021	Remote Services	Lateral-Movement
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/vulnerabilities-threats/maximum-severit...	T3

Source	URL	Tier
Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
CISA Issues Emergency Directive to Secure Cisco SD-WAN Systems	https://www.cisa.gov/news-events/news/immediate-action-required-cis...	T1
Cisco Catalyst SD WAN just got hit with active exploits ... - Reddit	https://www.reddit.com/r/sysadmin/comments/1rm660l/cisco_catalyst_s...	T3
Cisco SD-WAN - Security Advisories, Responses and Notices	https://www.cisco.com/c/en/us/support/routers/sd-wan/products-secur...	T3

Generated 2026-05-14 18:51 UTC by TJS Security Command Center