INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:32 UTC

Cisco Catalyst SD-WAN Manager: Two Additional CVEs Confirmed Exploited, Campaign Expanding [SCC-2026-0010]

CVE VULNERABILITY | HIGH | CVSS 5.4

SCC Item ID	SCC-CVE-2026-0006
Type	CVE Vulnerability
CVE ID	CVE-2026-20122, CVE-2026-20128
Severity	HIGH
CVSS Base Score	5.4
Affected Products	Cisco Catalyst SD-WAN Manager (vManage) — versions prior to 20.9.8.2, 20.12.5.3, 20.12.6.1, 20.15.4.2
Published	20260306

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm immediately if: (1) any vManage instance shows forensic evidence of successful CVE-2026-20122 exploitation (credential extraction or unauthorized API calls to user list endpoints in logs dated before notification), (2) any unexpected persistence mechanism detected (new admin accounts, modified cron jobs, SSH keys) post-patch, or (3) credential compromise suspected across DCA or downstream SD-WAN edge devices.
Recovery Notes	Post-containment: (1) Conduct full credential audit across all systems connected to vManage (DCA, edge routers, API consumers); reset any credentials that may have been exposed. (2) Review network flow logs for lateral movement from vManage to other management subnets — any unexpected East-West traffic warrants investigation of destination hosts. (3) Retain all audit logs, API request logs, and forensic snapshots for 1 year minimum to support forensic analysis if follow-up compromise is discovered.
Forensic Artifacts	/opt/csd/log/vmanage-audit.log (administrative actions, account changes, config writes) | /opt/csd/log/vmanage-api.log (API requests, authentication events, data access patterns) | /var/log/auth.log (SSH login attempts, service account authentication, privilege escalation) | vManage filesystem modification times and hash changes (pre- vs. post-patch /opt/vmanage directory trees, focus on /opt/vmanage/bin and /opt/vmanage/lib) | Network packet capture on port 443/8443 to vManage (TLS metadata, API endpoint access patterns, data exfiltration volume)

Per-Action IR Details

DETECT, Use Tenable ASM or internal inventory to identify all Cisco Catalyst SD-WAN Manager (vManage) instances.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: tools and resources)

Controls: NIST IR-4(1) incident handling capability, CIS 2.1 asset inventory

Compensating: Run 'nmap -p 443 --script ssl-cert ' to discover vManage instances by SSL certificate subject CN=vmanage; cross-reference with 'grep -r vmanage /etc/hosts /etc/resolv.conf' and DNS lookups. Export results to CSV for manual inventory tracking.

Evidence: Capture baseline network topology diagram and current asset inventory before discovery scan. Document timestamp of discovery scan execution. Preserve nmap output with -oA flag to capture all three formats (XML, greppable, normal).

CONTAIN, Review all accounts with API access to vManage, particularly read-only accounts that could enable CVE-2026-20122 exploitation. Disable unused accounts. Restrict management interface access to known-good hosts.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2 (containment strategies) and §3.2.4 (internal containment)

Controls: NIST AC-2 account management, NIST AC-3 access enforcement, CIS 5.2 privileged access management

Compensating: Export vManage user list via CLI: 'request admin user list' (or API: curl -k https:///dataservice/admin/users). Compare against business-justified access list (RACI matrix). Disable accounts via CLI: 'request admin user delete '. Restrict SSH/HTTPS access by adding vManage IP to network ACL permit-list only (e.g., 'access-list 101 permit tcp host host eq 443').

Evidence: Before disabling accounts, export full user list with 'request admin user list' and capture timestamps. Export vmanage audit logs: '/opt/csd/log/vmanage-audit.log'. Capture current SSH and HTTPS access control lists (show running-config | include access-list). Document each disabled account with justification and timestamp.

MITIGATE, Apply fixed releases: version 20.9.x → 20.9.8.2; version 20.12.x → 20.12.5.3 or 20.12.6.1; version 20.13–20.14 → 20.15.4. For CVE-2026-20128: versions 20.18 and later are not affected.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.3 (eradication) and §3.3.1 (removing the attacker's artifacts)

Controls: NIST SI-2 flaw remediation, CIS 7.2 ensure software is up to date

Compensating: If patch deployment is delayed, apply compensating controls: (1) Isolate affected vManage instances on a dedicated VLAN with no outbound internet access except approved update servers; (2) Implement network-based WAF rules to block POST requests to /dataservice/admin endpoints; (3) Disable API completely via vManage CLI: 'system service api disable' (then use SSH only for administration). Document compensating control start date and expected patch date.

Evidence: Before patching, capture full vManage filesystem snapshot: 'tar czf /backup/vmanage-pre-patch-$(date +%s).tar.gz /opt/vmanage /etc'. Export running configuration: 'request admin export'. Capture current version: 'show version | include vmanage-release'. Export active process list: 'ps auxww | grep -E vmanage|java|nginx > /backup/pre-patch-processes.txt'. Save system event log: 'show log install-log'.

VERIFY, After patching, rotate all vManage credentials and DCA service account passwords. Confirm no unexpected files were written to the SD-WAN Manager filesystem.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (recovery: return to normal operations) and §4.1 (lessons learned)

Controls: NIST IA-4 identifier management, NIST SI-7 software, firmware, and information integrity

Compensating: Manually rotate service account passwords via vManage UI (Admin > Users) and DCA service account via CLI: 'request admin dca password '. Verify account rotation in audit log: 'tail -f /opt/csd/log/vmanage-audit.log | grep password_changed'. For filesystem verification without EDR, use: 'find

/opt/vmanage /etc -type f -mtime -1 -ls | tee /audit/post-patch-new-files.log' to list files modified in past 24 hours. Compare against pre-patch snapshot with 'diff -r /backup/pre-patch-extract /opt/vmanage > /audit/filesystem-delta.txt'.

Evidence: Capture pre-rotation credential hashes (if stored): 'grep -A 5 admin /etc/vmanage/users.conf | md5sum'. Record password rotation timestamps from vmanage-audit.log. Export filesystem modification times before and after patching: 'stat /opt/vmanage/* | grep Modify'. Document any unexpected files with full metadata: 'ls -laR /opt/vmanage > /audit/post-patch-filesystem-manifest.txt'.

MONITOR, Alert on anomalous API calls from unfamiliar IPs or service accounts. Monitor for unexpected file modifications on vManage. Review CISA Emergency Directive 26-03 for detailed hunt guidance.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4.4 (monitoring and data retention after incident) and NIST IR-6 incident reporting

Controls: NIST SI-4 information system monitoring, NIST AU-2 audit events, CIS 8.5 log alerting

Compensating: Enable vManage API request logging: 'system settings logging level debug' (then parse /opt/csd/log/vmanage-api.log). Use grep-based alerting: 'grep -i 'api.*error\|auth.*fail\|unauthorized' /opt/csd/log/vmanage-api.log | mail -s vmanage-alert ops@company.com' (run hourly via cron). For file monitoring: 'auditctl -w /opt/vmanage -p wa -k vmanage_changes' (audit daemon) or fallback to daily cron job: 'find /opt/vmanage -type f -mtime -1 > /audit/daily-changes-$(date +%Y%m%d).log'. Parse CISA ED 26-03 for hunt rules and manually grep vManage logs for indicators: grep 'GET.*admin.*users\|POST.*config' /opt/csd/log/vmanage-api.log.

Evidence: Collect vmanage-api.log, vmanage-audit.log, and system syslog daily; retain for 90 days minimum. Enable audit on API endpoints: 'auditctl -w /opt/vmanage/api -p x -k api_execution'. Capture network traffic to vManage port 443 with tcpdump: 'tcpdump -i any -w /pcap/vmanage-$(date +%s).pcap port 443' (rotate weekly). Export service account login history: 'grep sshd /var/log/auth.log | grep -i accepted'.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`/dataservice/disasterrecovery/download/token`	REST API endpoint potentially targeted in Cisco SD-WAN vManage authentication bypass or information disclosure attempts	MEDIUM
URL	`/dataservice/client/server`	vManage REST API endpoint commonly probed during reconnaissance against Cisco SD-WAN infrastructure	MEDIUM
URL	`/dataservice/`	Base path for vManage REST API; unusual or unauthenticated access patterns to this path may indicate exploitation attempts	MEDIUM
FILE_PATH	`/opt/csm/web/assets/`	vManage web application asset directory; unexpected file creation here may indicate webshell deployment post-exploitation	MEDIUM
FILE_PATH	`/opt/csm/web/server/`	vManage server-side application directory; unauthorized modifications may indicate persistent access	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/var/log/nms/vmanage-server.log`	Primary vManage application log file; should be monitored for anomalous API call patterns, authentication failures, or error spikes	HIGH
FILE_PATH	`/var/log/nms/vmanage-aaa.log`	vManage AAA authentication log; critical for detecting unauthorized access attempts and authentication bypass activity	HIGH
FILE_PATH	`/etc/cron.d/`	Cron directory on vManage appliance; attackers may install persistence mechanisms here following exploitation	MEDIUM
FILE_PATH	`/tmp/`	Suspicious when vManage processes write executable files or scripts to /tmp/ outside of documented upgrade/patch procedures, as this directory is not part of legitimate application staging; legitimate operations use versioned directories under /opt/vmanage/ instead, so detect unexpected file creation, modification timestamps correlating with process execution anomalies, or presence of .sh/.py/.elf files in /tmp/ without corresponding maintenance tickets.	MEDIUM
REGISTRY_KEY	`N/A - Linux-based appliance`	Cisco vManage runs on a Linux-based OS; registry keys are not applicable. Focus on filesystem and process monitoring instead.	HIGH
FILE_PATH	`/home/admin/.ssh/authorized_keys`	SSH authorized keys file for admin account; attackers may add unauthorized public keys to maintain persistent SSH access	HIGH
URL	`/dataservice/settings/configuration/`	Configuration API endpoint; unauthorized access may indicate attempt to extract or modify SD-WAN configuration data	MEDIUM
URL	`/dataservice/template/`	Template management API endpoint; exploitation could allow unauthorized template modification affecting WAN policy	MEDIUM
FILE_PATH	`/usr/share/java/vmanage/`	vManage Java application directory; unexpected JAR files or modifications may indicate supply chain or post-exploitation tampering	MEDIUM

Type	Value	Context	Confidence
URL	`/dataservice/admin/user`	User management API endpoint; unauthorized calls to create or modify users may indicate privilege escalation following exploitation	HIGH

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1222** — File and Directory Permissions Modification
- **T1552.001** — Credentials In Files
- **T1078.003** — Local Accounts

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1222	File and Directory Permissions Modification	Defense-Evasion
T1552.001	Credentials In Files	Credential-Access

Technique ID	Technique Name	Tactic
T1078.003	Local Accounts	Defense-Evasion

Sources

Source	URL	Tier
Help Net Security, March 5, 2026	https://www.helpnetsecurity.com/2026/03/05/cisco-cve-2026-20128-cve...	T3
The Hacker News, March 5, 2026	https://thehackernews.com/2026/03/cisco-confirms-active-exploitatio...	T3
SecurityWeek, March 5, 2026	https://www.securityweek.com/cisco-warns-of-more-catalyst-sd-wan-fl...	T3
Tenable	https://www.tenable.com/blog/cve-2026-20127-cisco-catalyst-sd-wan-c...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20122, CVE-2026-20128	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3

Generated 2026-03-29 18:32 UTC by TJS Security Command Center