INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 18:52 UTC

Cisco Catalyst SD-WAN Manager - Cisco Catalyst SD-WAN Manager Exposure of Sensitive Information to an Unauthorized Actor Vulnerability

CVE VULNERABILITY | **HIGH** | CVSS 7.5 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0057
Type	CVE Vulnerability
CVE ID	CVE-2026-20133
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0007 (21th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability (due: 2026-04-23)
Affected Products	Cisco Catalyst SD-WAN Manager
Published	2026-04-20
Discovery Source	Cisa Kev

Executive Summary

A confirmed, actively exploited vulnerability in Cisco Catalyst SD-WAN Manager allows unauthenticated remote attackers to access sensitive system information without credentials. CISA has added this to its Known Exploited Vulnerabilities catalog, confirming real-world exploitation is occurring now. Organizations running Cisco SD-WAN infrastructure face immediate risk of network topology exposure, credential harvesting, and potential lateral movement across WAN-connected environments.

Technical Analysis

CVE-2026-20133 is an information disclosure vulnerability (CWE-200) in Cisco Catalyst SD-WAN Manager. The flaw permits unauthenticated remote actors to retrieve sensitive information from affected systems over the network without requiring prior authentication or elevated privileges. CVSS base score is 7.5 (High). CISA KEV remediation due date is 2026-04-23, confirming active exploitation. MITRE ATT&CK mappings include T1213 (Data from Information Repositories) and T1590 (Gather Victim Network Information), indicating adversaries are likely using exposed data for reconnaissance and pre-attack intelligence gathering. Refer to Cisco Security Advisory cisco-sa-sdwan-authbp-qwCX8D4v for authoritative affected version ranges; version details are not

repeated here to avoid duplication. CWE-200 class vulnerabilities in SD-WAN management planes carry elevated risk because exposed data typically includes routing configurations, peer relationships, and potentially credential artifacts. EPSS score is 0.00068 (20.9th percentile) as of scoring date, though KEV confirmation supersedes probabilistic scoring for prioritization purposes.

Action Checklist

1. Containment: Immediately restrict network access to Cisco Catalyst SD-WAN Manager interfaces. Block unauthenticated external access at the perimeter firewall and ensure management plane interfaces are not internet-facing. Verify no management ports are exposed on public IPs.
2. Detection: Query firewall and SD-WAN Manager access logs for unauthenticated or anomalous GET requests to management API endpoints. Look for unexpected source IPs accessing the management plane, particularly requests that return 200 status without authentication events. Correlate with T1590 reconnaissance patterns: repeated enumeration of network topology endpoints.
3. Eradication: Apply the Cisco-issued patch for CVE-2026-20133 as identified in the Cisco Security Advisory (sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v). Verify installed version against Cisco's confirmed fixed-version list. Do not rely on network-layer controls as the sole fix; patch the underlying software.
4. Recovery: After patching, audit SD-WAN Manager logs for evidence of prior unauthorized access. Rotate any credentials, API keys, or pre-shared keys that may have been exposed or accessible via the vulnerable interface. Revalidate SD-WAN peer configurations for unexpected changes.
5. Post-Incident: Review management plane exposure policy. SD-WAN Manager should never be internet-accessible without strong authentication controls. Implement control improvements aligned with NIST SP 800-53 AC-17 (Remote Access) and SC-7 (Boundary Protection). Consider adding this class of vulnerability to your next threat model review cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if log analysis confirms unauthorized access to vManage API endpoints during the exploitation window, as exposed SD-WAN topology, device credentials, or pre-shared keys constitute a potential data breach with regulatory notification obligations; also escalate if the vManage instance serves multi-tenant or third-party WAN environments, expanding the blast radius beyond the immediate organization.
Recovery Notes	After patching CVE-2026-20133 and rotating credentials, monitor the vManage audit log (`/var/log/nms/audit.log`) and SD-WAN peer device syslogs daily for a minimum of 30 days for indicators of post-exploitation activity — specifically unauthorized template modifications, new device onboarding events, or OMP routing policy changes that could indicate an attacker pre-positioned using topology data harvested during the exposure window. Revalidate all SD-WAN tunnel peer configurations (IPsec SAs, TLOC identities, and VPN segment assignments) against your last known-good configuration backup to confirm no unauthorized changes were introduced. If any SD-WAN-connected remote sites have independent security monitoring, notify their security teams of the exposure window so they can independently review lateral movement indicators sourced from WAN-side traffic.

Forensic Artifacts	vManage NMS server access log (`/var/log/nms/vmanage-server.log`): contains timestamped HTTP request records for all REST API calls to `/dataservice/` endpoints — the primary artifact for identifying unauthenticated 200-status responses to topology, device, and template endpoints that constitute the CVE-2026-20133 exploitation pattern | vManage NMS audit log (`/var/log/nms/audit.log`): records all authenticated configuration changes with user attribution — cross-reference against the access log to identify API activity in the exploitation window that lacks a corresponding authenticated session, confirming unauthorized access per the vulnerability mechanism | Perimeter firewall connection logs for destination ports 443, 8443, and 8080 to the SD-WAN Manager IP(s): provides source IP attribution, session duration, and data transfer volume for all external connections — critical for determining whether reconnaissance (repeated small GETs consistent with T1590 enumeration) or bulk data exfiltration of topology/config data occurred | SD-WAN Manager configuration database export (`request nms configuration-db backup` or Administration > Backup): captures the full device template inventory, VPN segmentation policies, and OMP routing configurations at a point-in-time — diff against a pre-incident backup to detect any unauthorized configuration modifications introduced during or after the exploitation window | vManage API key and user session records (`GET /dataservice/admin/user` and `GET /dataservice/admin/token` via authenticated API post-patch): documents all API tokens issued during the exploitation window that may have been created by or revealed to an unauthorized actor, and identifies which accounts had active sessions concurrent with anomalous unauthenticated access events

Per-Action IR Details

Containment — Immediately restrict network access to Cisco Catalyst SD-WAN Manager interfaces. Block unauthenticated external access at the perimeter firewall and ensure management plane interfaces are not internet-facing. Verify no management ports are exposed on public IPs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further unauthorized access while preserving forensic state

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On the perimeter firewall (iptables/nftables or Cisco ASA ACL), immediately block inbound TCP to SD-WAN Manager default ports 443, 8443, and 8080 from any source outside the defined management VLAN. Run: `netstat -tlnp | grep -E '443|8443|8080'` on the SD-WAN Manager host to enumerate all listening sockets. Use `ss -tnp state established` to capture any currently active connections before blocking — document these as forensic artifacts. If using a Cisco ASA, apply an ACL deny entry to the outside interface for destination IPs hosting the SD-WAN Manager before broader changes.

Evidence: Before implementing firewall blocks, capture the full current connection table from the SD-WAN Manager host (`ss -tnp` or `netstat -anp`) to preserve any active unauthorized sessions. Export the perimeter firewall session table and NAT translation table to identify whether management ports (443, 8443, 8080) are currently published to public IPs. Pull SD-WAN Manager system logs from `/var/log/nms/` (vManage log directory) to baseline the current access state before containment alters traffic patterns.

Detection — Query firewall and SD-WAN Manager access logs for unauthenticated or anomalous GET requests to management API endpoints. Look for unexpected source IPs accessing the management plane, particularly requests that return 200 status without authentication events. Correlate with T1590 reconnaissance patterns: repeated enumeration of network topology endpoints.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to establish scope of unauthorized access to the SD-WAN management plane

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Query the vManage access log at `/var/log/nms/vmanage-server.log` and the NMS audit log at `/var/log/nms/audit.log` using: `grep -E 'GET .*(dataservice|template|device|topology)' /var/log/nms/vmanage-server.log | grep ' 200 ' | awk '{print $1, $2, $7, $9}' | sort | uniq -c | sort -rn` to surface high-frequency 200-status responses to management API paths without corresponding auth events. Cross-reference source IPs against your known management VLAN range. For firewall logs (if syslog-forwarded to a local file), run: `grep -E '(443|8443|8080)' /var/log/firewall.log | awk '{print $NF}' | sort | uniq -c | sort -rn` to rank external source IPs by access frequency. Flag any IP appearing with >10 API requests lacking a preceding POST to `/j_security_check` (the vManage authentication endpoint).

Evidence: Collect the full vManage NMS server log (`/var/log/nms/vmanage-server.log`) and audit log (`/var/log/nms/audit.log`) covering at minimum 30 days prior to detection, preserving original timestamps (NIST AU-8). Extract HTTP access log entries showing requests to REST API paths under `/dataservice/` — particularly `/dataservice/network/issues`, `/dataservice/device`, `/dataservice/template/feature`, and `/dataservice/topology/` — that returned HTTP 200 without a preceding session authentication event. Capture source IP, timestamp, HTTP method, URI, response code, and response body size for each anomalous request to establish MITRE ATT&CK T1590 (Gather Victim Network Information) reconnaissance scope.

Eradication — Apply the Cisco-issued patch for CVE-2026-20133 as identified in the Cisco Security Advisory (sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v). Verify installed version against Cisco's confirmed fixed-version list. Do not rely on network-layer controls as the sole fix — patch the underlying software.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remediate the root cause vulnerability in Cisco Catalyst SD-WAN Manager by applying the vendor-issued software fix, not solely network compensating controls

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CM-3 (Configuration Change Control), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before patching, snapshot the current vManage version with: `vmanage$ show version` (vManage CLI) or via REST API: `curl -sk -b cookies.txt https:///dataservice/version` (authenticated). Document the pre-patch version string as a forensic baseline. After applying the Cisco-supplied upgrade package per the advisory procedures, re-run the version check and diff against Cisco's fixed-version list published in the advisory. Use `rpm -qa | grep -i vmanage` or the equivalent package manager query on the underlying OS to verify package replacement. If patching must be deferred beyond 24 hours due to change control, ensure the network-layer ACL from the Containment step remains enforced and document the exception with a dated compensating control record per NIST SI-2.

Evidence: Before initiating the patch, capture a full configuration export from vManage (Administration > Backup/Restore or `request nms configuration-db backup path `) to establish a pre-patch forensic baseline. Record the exact installed software version, build number, and package checksums. After patching, retain the upgrade log (`/var/log/nms/install.log` or equivalent) as evidence of remediation for audit purposes per NIST SI-2 and CIS 7.2. Note: the advisory URL provided in the action step should be validated directly against Cisco's Security Advisory portal at sec.cloudapps.cisco.com — treat it as a reference pointer requiring human confirmation before use, consistent with GAIO URL policy.

Recovery — After patching, audit SD-WAN Manager logs for evidence of prior unauthorized access. Rotate any credentials, API keys, or pre-shared keys that may have been exposed or accessible via the vulnerable interface. Revalidate SD-WAN peer configurations for unexpected changes.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore SD-WAN infrastructure to a verified secure state, confirm integrity of peer configurations, and rotate all credentials potentially exposed through the unauthorized information

disclosure

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: Enumerate all vManage local accounts and API tokens via: `vmanage# show aaa users` (CLI) or REST API: `GET /dataservice/admin/user` (authenticated post-patch). For each account, check last-login timestamps in the audit log (`/var/log/nms/audit.log`) against expected usage patterns — flag any account with API activity during the suspected exploitation window. Rotate all vManage admin passwords, API tokens (revoke via Administration > API Keys), and IPsec/TLS pre-shared keys used in SD-WAN tunnel configurations. Export the current vEdge/cEdge device template and peer configuration list (`GET /dataservice/template/device`) and diff against your last known-good configuration backup to detect unauthorized topology or policy modifications.

Evidence: Pull and preserve the vManage audit log covering the full window from earliest possible exploitation (first anomalous API access identified in Detection step) through patch application, as this log records all configuration changes with user attribution per NIST AU-10 (Non-Repudiation). Extract all API key issuance and revocation events. Document any SD-WAN peer configuration (device templates, VPN segmentation policies, OMP route policies) that was modified or could have been read during the unauthorized access window — network topology data exposed via this CVE could be used to pre-position for lateral movement across WAN-connected sites (MITRE ATT&CK T1590.005 — IP Addresses).

Post-Incident — Review management plane exposure policy. SD-WAN Manager should never be internet-accessible without strong authentication controls. Implement control improvements aligned with NIST SP 800-53 AC-17 (Remote Access) and SC-7 (Boundary Protection). Consider adding this class of vulnerability to your next threat model review cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update network segmentation and management plane access policies, and integrate SD-WAN management exposure as a standing threat model item

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Document the lessons-learned findings specific to this incident: (1) whether the SD-WAN Manager management interface was reachable from outside the management VLAN and why, (2) how long the exposure existed before detection, and (3) whether Cisco security advisory monitoring (PSIRT RSS feed or Cisco Security Advisory email subscription) would have triggered earlier patching. Update your network segmentation diagram to formally designate the SD-WAN Manager management plane as a Restricted Zone per SC-7. Add a recurring quarterly check — scriptable as: `nmap -p 443,8443,8080 --open` run from an external vantage point — to detect future management plane re-exposure. Subscribe to the Cisco PSIRT advisory feed (tools.cisco.com/security/center/rss.x) to ensure future SD-WAN Manager advisories trigger your patch triage workflow within 24 hours of publication.

Evidence: Compile the complete incident timeline from first possible exposure through recovery completion, citing specific log timestamps from the vManage audit log and firewall logs collected during Detection and Recovery phases. Retain all forensic artifacts (log exports, configuration diffs, credential rotation records) for a minimum period consistent with your organization's audit record retention policy per NIST AU-11 (Audit Record Retention) — typically 1–3 years. Document whether the CVE-2026-20133 exploitation window resulted in any confirmed data exfiltration of network topology, device configurations, or credentials, as this determination drives breach notification obligations and should be included in the post-incident report per NIST IR-8.

Detection Guidance

Focus detection on the SD-WAN Manager access logs and upstream firewall/proxy logs. Look for: unauthenticated HTTP/HTTPS requests to SD-WAN Manager API endpoints that return non-error responses; source IPs with no prior authentication events making repeated requests to configuration or status endpoints; unusual volume of outbound data from the SD-WAN Manager host following unauthenticated requests. MITRE T1590 (network reconnaissance) pattern: sequential enumeration of peer, route, or topology endpoints from a single external source. MITRE T1213 pattern: bulk retrieval of repository or configuration data. If your SIEM ingests Cisco SD-WAN Manager logs, create an alert on successful API responses (HTTP 200) where no corresponding authentication event exists for the source IP within the session window.

Framework Mappings

MITRE-ATTACK

- **T1213** — Data from Information Repositories
- **T1590** — Gather Victim Network Information

OWASP-TOP10-2021

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

NIST-800-53R5

- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest
- **IR-5** — Incident Monitoring

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

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
T1213	Data from Information Repositories	Collection
T1590	Gather Victim Network Information	Reconnaissance

Sources

Source	URL	Tier
cisa_kev	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Source	URL	Tier
CVE-2026-20133 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20133	T1
Vulnerability Details : CVE-2026-20133 - Cisco	https://www.cvedetails.com/cve/CVE-2026-20133/	T3
CVE-2026-20133 - Red Hat Customer Portal	https://access.redhat.com/security/cve/cve-2026-20133	T3
Cisco Catalyst SD-WAN Vulnerabilities	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-04-20 18:52 UTC by TJS Security Command Center