INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 13:49 UTC

Cisco Catalyst SD-WAN Authentication Bypass (CVE-2026-20182), CVSS 10.0, Active Exploitation, No Workarounds

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0178
Type	CVE Vulnerability
CVE ID	CVE-2026-20182
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Cisco Catalyst SD-WAN Controller (formerly SD-WAN vSmart) and Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage), all deployment types: On-Prem, SD-WAN Cloud-Pro, Cisco Managed Cloud, SD-WAN for Government (FedRAMP)
Published	2026-05-14T16:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A maximum-severity authentication bypass vulnerability (CVE-2026-20182) in Cisco Catalyst SD-WAN Controller and Manager allows unauthenticated remote attackers to seize full administrative control over an organization's SD-WAN fabric. All deployment types are affected, including on-premises, cloud, and FedRAMP environments, with no available workarounds; patching is the only remediation path. Cisco has confirmed limited active exploitation, CISA has issued Emergency Directive ED-26-03, and a related SD-WAN zero-day (CVE-2026-20127) has been exploited by threat actor UAT-8616 since at least 2023, indicating a sustained, targeted campaign against this infrastructure.

Technical Analysis

CVE-2026-20182 is an improper authentication flaw (CWE-287) in the NETCONF interface of Cisco Catalyst SD-WAN Controller (formerly vSmart) and Cisco Catalyst SD-WAN Manager (formerly vManage). Cisco title materials reference CVSS 10.0; however, this item's severity.cvss_base field contains 9.5. Defer to the official Cisco Security Advisory (cisco-sa-sdwan-rpa2-v69WY2SW) for the authoritative CVSS score. All deployment models are affected: On-Prem, SD-WAN Cloud-Pro, Cisco Managed Cloud, and SD-WAN for Government (FedRAMP). An unauthenticated remote attacker can exploit this flaw over the network without user interaction to gain administrative privileges and manipulate SD-WAN fabric configuration, covering routing policy,

segmentation, and control plane behavior. CWE-22 (Path Traversal) is also listed as a weakness; its precise role in the exploit chain is not fully characterized in available source data. Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1548 (Abuse Elevation Control Mechanism), T1556 (Modify Authentication Process), T1098 (Account Manipulation), T1059 (Command and Scripting Interpreter), T1565 (Data Manipulation), T1133 (External Remote Services), T1562 and T1562.010 (Impair Defenses). A related zero-day, CVE-2026-20127, has been exploited by UAT-8616 since at least 2023 (3+ years of documented activity). No workarounds exist. Cisco has confirmed limited active exploitation as of May 2026. CISA Emergency Directive ED-26-03 and an NSA/ACSC joint advisory are in effect.

Action Checklist

1. Step 1: Containment, Immediately identify all Cisco Catalyst SD-WAN Controller (vSmart) and SD-WAN Manager (vManage) instances across all deployment types (On-Prem, SD-WAN Cloud-Pro, Cisco Managed Cloud, FedRAMP). Restrict NETCONF access (TCP port 830) to trusted management IPs via ACLs or firewall rules as a temporary exposure reduction measure; this is a defense-in-depth control and does not replace vendor patching. Treat any SD-WAN Manager or Controller exposed to untrusted networks as potentially compromised pending patch verification. Reference Cisco Security Advisory cisco-sa-sdwan-rpa2-v69WY2SW for affected software versions.
2. Step 2: Detection, Review NETCONF session logs on SD-WAN Manager and Controller for authentication events from unexpected source IPs, sessions established without corresponding valid credential events, and administrative configuration changes (policy, routing, segmentation) not initiated by known change records. Cross-reference SD-WAN Manager audit logs for privilege escalation events, new account creation (T1098), and changes to authentication configurations (T1556). Check for indicators associated with UAT-8616 activity; consult the NSA/ACSC joint advisory (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4416296/) for published IOCs and hunting guidance. EPSS data was not available in source data at time of publication; monitor NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-20182) for updates.
3. Step 3: Eradication, Apply the patch specified in Cisco Security Advisory cisco-sa-sdwan-rpa2-v69WY2SW immediately. No workarounds exist; version upgrade is the only remediation path. Prioritize internet-facing and government (FedRAMP) deployments. After patching, rotate all SD-WAN Manager and Controller administrative credentials, revoke any sessions active during the exposure window, and audit all configuration changes made during that period for unauthorized modifications.
4. Step 4: Recovery, After patching, verify SD-WAN Manager and Controller are running the remediated software version per the Cisco advisory. Validate SD-WAN fabric configuration integrity, compare current routing policy, segmentation rules, and control plane settings against last known-good baselines. Monitor NETCONF session logs and administrative audit trails continuously for 30 days post-patch for signs of persistent access (T1078, T1133). Confirm CISA ED-26-03 reporting obligations are met within the directive's specified timeline.
5. Step 5: Post-Incident, Review NETCONF exposure posture across all network management interfaces, not only SD-WAN. Assess whether management plane access controls (zero-trust network access to admin interfaces, out-of-band management networks) would have limited the attack surface. Document exposure window and any detected unauthorized configuration changes for regulatory and insurance reporting. Given UAT-8616's sustained targeting of Cisco SD-WAN since 2023, evaluate whether threat hunting for earlier-stage intrusion activity is warranted across the broader network infrastructure.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if vManage audit logs show any NETCONF session established from a non-management IP during the exposure window, any unauthorized account creation or authentication configuration change is detected, or if the organization operates FedRAMP-authorized SD-WAN deployments subject to CISA ED-26-03's mandatory reporting timeline.
Recovery Notes	After patching, perform a full OMP (Overlay Management Protocol) routing table audit across all SD-WAN edge devices using 'show sdwan omp routes' — UAT-8616 has demonstrated capability to inject persistent rogue routes into the control plane that survive Controller restarts, so baseline comparison against pre-incident topology exports is essential. Monitor vManage administrative audit logs and NETCONF session logs at 15-minute intervals for a minimum of 30 days post-patch, with particular attention to any new API key issuance, certificate enrollment events, or control policy modifications, which may indicate attacker persistence via T1078 (Valid Accounts) or T1133 (External Remote Services). For FedRAMP deployments, do not declare recovery complete until CISA ED-26-03 reporting obligations are fulfilled and a Cisco TAC-verified clean-build attestation is obtained for all affected Controller and Manager nodes.
Forensic Artifacts	vManage Audit Log (Monitor > Audit Log or /dataservice/auditlog API): Contains timestamped records of every administrative action including login events, user creation, policy changes, and certificate operations — authentication bypass exploitation will appear as successful admin-level sessions without corresponding valid credential challenge events, distinguishable by missing MFA or RADIUS/TACACS validation log entries preceding the session. | SD-WAN Controller NETCONF Session Records (/var/log/messages and 'show netconf-yang sessions detail'): Logs every NETCONF session establishment including client IP, session ID, and duration — exploitation of CVE-2026-20182 will produce sessions from non-management IPs with admin-level YANG RPC operations (edit-config, get-config targeting /native/aaa or /native/interface paths) appearing without a preceding SSH authentication success record from the same source IP. | vManage PostgreSQL Database — audit_log and user tables (/var/lib/vmanage/data or accessed via 'psql -U vmanage'): Stores persistent change history for all configuration objects including routing policy, VPN segmentation, and user accounts — query for rows with entry_time within the exposure window and log_module values of 'policy', 'userManagement', or 'certificate' to identify attacker-introduced configuration modifications that may not appear in the UI audit log if log tampering occurred. | SD-WAN Edge Device OMP Route Tables ('show sdwan omp routes' on all vEdge/cEdge devices): An attacker with full SD-WAN Manager administrative access via this bypass can inject rogue OMP control plane routes to redirect traffic — compare current OMP routing tables against pre-incident topology exports for any route entries with unexpected next-hops, unexpected originator site-IDs, or routes for prefixes not present in approved network documentation. | Network Flow Records (NetFlow/IPFIX from SD-WAN edge interfaces during exposure window): UAT-8616 has historically used compromised SD-WAN infrastructure as a pivot point for lateral movement and data exfiltration — collect flow records from all cEdge/vEdge WAN interfaces for the exposure window and hunt for flows destined to non-documented external IPs on management ports (TCP/830, TCP/443, TCP/22) originating from the SD-WAN Controller or Manager management interfaces, which would indicate the attacker using the compromised fabric for C2 or exfiltration.

Per-Action IR Details

Step 1: Containment — Immediately identify all Cisco Catalyst SD-WAN Controller (vSmart) and SD-WAN Manager (vManage) instances across all deployment types (On-Prem, SD-WAN Cloud-Pro, Cisco Managed Cloud, FedRAMP). Restrict NETCONF access (TCP port 830) to trusted management IPs via ACLs or firewall rules as a temporary exposure reduction measure — note this is not a vendor-documented workaround and does not fully mitigate risk. Treat any SD-WAN Manager or Controller exposed to untrusted networks as potentially compromised pending patch verification. Reference Cisco Security Advisory cisco-sa-sdwan-rpa2-v69WY2SW for affected software versions.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 12.2 (Establish and Maintain a Secure Network Architecture)

Compensating: On each SD-WAN Manager and Controller node, immediately apply an ACL to drop inbound TCP/830 (NETCONF) from any source not in your documented management IP list. On IOS-XE-based controllers, use: 'ip access-list extended BLOCK-NETCONF / deny tcp any any eq 830 / permit ip any any' applied inbound on all untrusted interfaces. For perimeter firewalls (iptables-based Linux): 'iptables -I INPUT -p tcp --dport 830 -j DROP' with explicit permits for management IPs added first. Run 'netstat -tnp | grep :830' on each node to confirm no active unexpected NETCONF sessions exist before applying the ACL. Document every IP currently holding an active session as a potential attacker IP for Step 2 hunting.

Evidence: Before restricting access, capture the full list of currently active NETCONF sessions via 'show netconf-yang sessions detail' on IOS-XE SD-WAN Controller nodes, or the equivalent REST API call to vManage (/dataservice/management/session) — these session records will be overwritten when sessions are terminated. Also capture SD-WAN Manager's /var/log/nms/vmanage-server.log and the Controller's system syslog (/var/log/messages) to preserve authentication event history prior to ACL enforcement. Snapshot the current running configuration of all affected nodes using 'show running-config' before any changes — this serves as the baseline for post-eradication comparison.

Step 2: Detection — Review NETCONF session logs on SD-WAN Manager and Controller for authentication events from unexpected source IPs, sessions established without corresponding valid credential events, and administrative configuration changes (policy, routing, segmentation) not initiated by known change records. Cross-reference SD-WAN Manager audit logs for privilege escalation events, new account creation (T1098), and changes to authentication configurations (T1556). Check for indicators associated with UAT-8616 activity; consult the NSA/ACSC joint advisory (https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4416296/) for published IOCs and hunting guidance. EPSS data was not available in source data at time of publication — monitor NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-20182) for updates.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, perform targeted log extraction directly on SD-WAN Manager using the vManage audit log API: 'curl -k -X GET https:///dataservice/auditlog?query={\"query\":{\"condition\":\"AND\",\"rules\":[{\"field\":\"log module\",\"type\":\"string\",\"value\":[\"login\"],\"operator\":\"in\"}]}}' — pipe output through 'jq' to filter for entries where 'loguser' is not in your known admin account list or 'activity' contains 'Create User' or 'Modify Auth'. For Controller nodes, parse /var/log/messages with: 'grep -E "netconf|authenticated|session" /var/log/messages | grep -v "'". Use Zeek (free) on a tap/span port upstream of the SD-WAN Manager to capture and decode NETCONF over SSH (TCP/830) sessions — Zeek's ssh.log will show client IPs and session durations that can be cross-referenced against change records.

Evidence: Collect SD-WAN Manager audit logs from the vManage web UI (Monitor > Audit Log) or API export covering the full exposure window, filtered for modules: 'login', 'userManagement', 'policy', 'device', and 'certificate' — these will show unauthenticated bypass sessions appearing as successful logins without preceding credential validation events. On Controller nodes, extract NETCONF session establishment records from /var/log/messages filtering on 'subsystem: netconf'. Pull the SD-WAN Manager's PostgreSQL database audit tables (vmanage-server stores config change history) — query the 'audit_log' table for rows where 'entry_time' falls within the exposure window and 'log_module' = 'policy' or 'routing', as UAT-8616 has historically modified SD-WAN routing policy and segmentation rules to enable lateral movement across the fabric.

Step 3: Eradication — Apply the patch specified in Cisco Security Advisory cisco-sa-sdwan-rpa2-v69WY2SW immediately. No workarounds exist — version upgrade is the only remediation path. Prioritize internet-facing and government (FedRAMP) deployments. After patching, rotate all SD-WAN Manager and Controller administrative credentials, revoke any sessions active during the exposure window, and audit all configuration changes made during that period for unauthorized modifications.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-3 (Configuration Change Control), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Download the remediated SD-WAN software image directly from Cisco Software Download (software.cisco.com) — verify the SHA-512 hash published in cisco-sa-sdwan-rpa2-v69WY2SW against the downloaded image using 'sha512sum ' before staging. For FedRAMP deployments, coordinate image transfer through Cisco's FedRAMP-authorized delivery mechanism and document chain of custody. After upgrade, force credential rotation using the vManage API: 'POST /dataservice/admin/user/password/' for each admin account — automate across all accounts with a bash loop against the user list exported from '/dataservice/admin/user'. Revoke all active sessions via vManage: 'POST /dataservice/admin/user/denyaccess' or through the UI (Administration > Manage Users > Invalidate Sessions). For on-prem Controller nodes, use 'request platform software system reset' only after confirming patched image is staged to avoid downtime loops.

Evidence: Before applying the patch, take a full configuration archive from vManage (Tools > Operational Commands > Generate Bootstrap Configuration for each device) and export the complete configuration database backup (Administration > Disaster Recovery > Export) — this preserves the forensic state of any attacker-modified configurations for post-incident analysis. Capture 'show version' and 'show install summary' output from all Controller nodes pre-patch to document the vulnerable version as evidence. If any unauthorized accounts were created (detected in Step 2), do not delete them before extracting their full creation metadata — last login time, source IP, and any API keys issued — from the vManage audit log and PostgreSQL user table.

Step 4: Recovery — After patching, verify SD-WAN Manager and Controller are running the remediated software version per the Cisco advisory. Validate SD-WAN fabric configuration integrity — compare current routing policy, segmentation rules, and control plane settings against last known-good baselines. Monitor NETCONF session logs and administrative audit trails continuously for 30 days post-patch for signs of persistent access (T1078, T1133). Confirm CISA ED-26-03 reporting obligations are met within the directive's specified timeline.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST CM-6 (Configuration Settings), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Verify remediated version on all nodes with 'show version | include Software' on Controller nodes and check vManage UI (Administration > Software Repository > Current Version). For configuration integrity comparison, use the vManage Configuration diff tool (Configuration > Templates > Device Configuration > Diff) against a pre-incident backup — if no baseline exists, compare against your organization's last approved change ticket. For the

30-day monitoring period without a SIEM, deploy a cron job on a dedicated Linux monitoring host that runs every 15 minutes: 'curl -k -s https:///dataservice/auditlog | jq ".data[] | select(.entry_time >)" >> /var/log/sdwan-postpatch-audit.log' — alert on any entries where 'logmodule' is 'userManagement' or 'policy'. For CISA ED-26-03 reporting, use the CISA CIRCIA reporting portal and document the exposure window, affected deployment types, and patch completion timestamp.

Evidence: After patching, run 'show netconf-yang sessions' on all Controller nodes and confirm zero sessions from non-management IPs — capture this output as the clean-state baseline. Export the current SD-WAN fabric topology from vManage (Monitor > Network > Topology) and compare VPN segment assignments, control policy, and data policy against the pre-incident backup to identify any attacker-introduced routing changes — UAT-8616 has previously inserted rogue OMP route advertisements to redirect traffic through attacker-controlled nodes. Document 'show running-config' from all Controllers post-patch as the verified clean configuration for future baseline comparisons.

Step 5: Post-Incident — Review NETCONF exposure posture across all network management interfaces, not only SD-WAN. Assess whether management plane access controls (zero-trust network access to admin interfaces, out-of-band management networks) would have limited the attack surface. Document exposure window and any detected unauthorized configuration changes for regulatory and insurance reporting. Given UAT-8616's sustained targeting of Cisco SD-WAN since 2023, evaluate whether threat hunting for earlier-stage intrusion activity is warranted across the broader network infrastructure.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST AU-11 (Audit Record Retention), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Conduct a NETCONF/RESTCONF exposure audit across all Cisco infrastructure (routers, switches, wireless controllers) by scanning your management network with: 'nmap -p 830,832 --open ' — document every device responding on TCP/830 and verify each has management-plane ACLs restricting access to jump hosts only. For the UAT-8616 broader hunting assessment, use publicly available Sigma rules targeting Cisco SD-WAN NETCONF abuse (search the SigmaHQ GitHub repository for 'vmanage' or 'netconf' rules) and run them against archived logs. For regulatory documentation, structure your incident timeline using NIST IR-6 reporting format — exposure window start (first vulnerable version in production), exposure window end (patch applied timestamp), confirmed vs. unconfirmed compromise indicators, and all configuration changes detected during the window. Retain all SD-WAN Manager logs and database exports for a minimum of 3 years to meet FISMA/FedRAMP audit requirements.

Evidence: Archive the complete vManage audit log export, all NETCONF session logs from Controller nodes, the pre- and post-patch configuration snapshots, and any PostgreSQL database extracts from the incident window — store these in write-once storage (AWS S3 Object Lock, Azure Immutable Blob, or a WORM drive) to preserve forensic integrity per NIST AU-9 (Protection of Audit Information). For UAT-8616 hunting, collect NetFlow or IPFIX records from SD-WAN edge routers (vEdge/cEdge) for the exposure window — UAT-8616 has historically exfiltrated routing table data and used compromised SD-WAN fabric as a pivot point, so look for unexpected inter-VPN traffic flows or new BGP peer establishments that postdate the earliest possible exploitation timestamp.

Detection Guidance

Primary detection focus: unauthorized NETCONF sessions and administrative configuration changes on Cisco Catalyst SD-WAN Controller and Manager. Query SD-WAN Manager audit logs for: (1) administrative sessions with no corresponding authentication success event, (2) configuration changes outside approved change windows, (3) new user or role creation events (T1098), (4) modifications to authentication or policy settings (T1556), (5) NETCONF sessions from IPs not in the management ACL. At the network layer, inspect traffic logs for NETCONF (TCP/830) connections to SD-WAN Controller or Manager from untrusted or unexpected sources. For threat actor UAT-8616 behavioral indicators and specific IOCs, consult the NSA/ACSC joint advisory published at

https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4416296/, which includes hunting guidance specific to the broader SD-WAN campaign. No CVE-specific IOCs (hashes, IPs, domains) were confirmed in the available source data at publication; consult threat intelligence feeds for updates, and do not assume unlisted indicators are insignificant. Monitor the CISA ED-26-03 directive page (https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems) for updated IOC guidance.

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1562.010** — Downgrade Attack
- **T1562** — Impair Defenses
- **T1556** — Modify Authentication Process
- **T1133** — External Remote Services
- **T1078** — Valid Accounts
- **T1059** — Command and Scripting Interpreter
- **T1565** — Data Manipulation
- **T1098** — Account Manipulation
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **AU-9** — Protection of Audit Information
- **SI-4** — System Monitoring
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

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
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1562.010	Downgrade Attack	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion
T1556	Modify Authentication Process	Credential-Access
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution

Technique ID	Technique Name	Tactic
T1565	Data Manipulation	Impact
T1098	Account Manipulation	Persistence
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T3
	https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Rele...	T1
	https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulne...	T1
	https://www.helpnetsecurity.com/2026/02/25/cisco-sd-wan-zero-day-cv...	T3
CVE-2026-2018 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-2018	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-20182	T1
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecuri...	T1

Generated 2026-05-14 13:49 UTC by TJS Security Command Center