NCA-08.060326 – National CERT Advisory

Critical Authentication Bypass in Cisco Systems Catalyst SD-WAN Manager (CVE-2026-20127)

A critical authentication bypass vulnerability has been identified in Cisco Systems Catalyst SD-WAN Manager (vManage), tracked as **CVE-2026-20127**. The vulnerability carries a **CVSS score of 10.0 (Critical)** and is confirmed to have been exploited in zero-day attacks targeting internet-exposed SD-WAN management interfaces.

The flaw allows a remote, unauthenticated attacker to bypass authentication controls and gain administrative-level access to affected systems. Given the centralized control function of SD-WAN controllers, successful exploitation may result in full network compromise, configuration manipulation, credential harvesting, lateral movement, operational disruption, and long-term persistence within enterprise environments.

Immediate remediation is required for all affected deployments.

DOCUMENT SUMMARY

Advisory ID	NCA-02.260226
Threat Type	Authentication Bypass / Remote Administrative Compromise
Severity	**Critical**
Attack Vector	Network (Remote)
Authentication Required	No
User Interaction	None
CVSS Score	10.0 (Critical – Full System Compromise)
CVE ID	CVE-2026-20127
Affected Product	Cisco Catalyst SD-WAN Manager

IMPACT ANALYSIS

Successful exploitation may result in:

1. **Unauthenticated Administrative Access** – Complete bypass of login controls
2. **Full SD-WAN Infrastructure Compromise** – Centralized control over WAN orchestration
3. **Arbitrary Command Execution** – Execution of system-level commands
4. **Rogue Account Creation** – Persistent unauthorized administrative access
5. **Configuration Manipulation** – Malicious modification of routing, segmentation, or security policies
6. **Sensitive Data Extraction** – Exposure of network configurations, credentials, certificates, and API tokens
7. **Enterprise Network Pivoting** – Lateral movement into managed branch and data center environments
8. **Operational Disruption** – Network outages or traffic interception
9. **Long-Term Persistence** – Establishment of backdoor access through controller compromise
10. **National Critical Infrastructure Risk** – Potential impact to government and regulated sectors using SD-WAN for core connectivity

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Remote Authentication Bypass
Threat Status	Actively Exploited (Zero-Day)

Root Cause	Improper validation of authentication requests in web management interface
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Exposure Risk	Highest where vManage interface is internet-facing
Affected Deployments	Physical and virtual SD-WAN Manager installations
CWE Classifications	CWE-287 (Improper Authentication), CWE-306 (Missing Authentication for Critical Function), CWE-284 (Improper Access Control)

AFFECTED SYSTEMS

- Cisco Catalyst SD-WAN Manager versions prior to Cisco security-fixed releases
- Internet-exposed SD-WAN management interfaces
- Clustered and high-availability deployments (all nodes must be updated)
- Both physical and virtual appliances
- Also affects Cisco Catalyst SD-WAN Controller (formerly vSmart)

Organizations must consult Cisco's official advisory for exact affected release trains and patched versions.

INDICATORS OF COMPROMISE (IoCs)

1. Unexpected creation of new administrative accounts
2. Authentication logs showing successful logins without valid credential events
3. Unrecognized configuration changes in SD-WAN policies or device templates
4. Unexpected API token generation or privilege escalation
5. Suspicious outbound traffic originating from vManage systems
6. Evidence of lateral movement from SD-WAN management infrastructure
7. Log anomalies around web authentication endpoints
8. Disabled or modified logging configurations
9. Unexpected device re-enrollment or certificate changes
10. Indicators of web exploitation activity targeting management interface URLs

REMEDIATION ACTIONS

Action Category	Specific Actions	Priority
Immediate Patching	Upgrade to Cisco's fixed SD-WAN software versions	**MANDATORY**
Exposure Reduction	Remove direct internet exposure of vManage interfaces	**MANDATORY**
Access Control	Restrict management access via strict IP allowlisting and firewall policies	HIGH
Cluster Integrity	Verify all nodes in HA/clustered deployments are patched	HIGH
Post-Patch Audit	Review administrative accounts, API tokens, and configuration integrity	REQUIRED
Credential Hygiene	Rotate credentials, certificates, and API keys as precaution	REQUIRED
Monitoring	Increase logging and real-time alerting on SD-WAN systems	REQUIRED
CISA Emergency Directive	"CISA Emergency Directive ED 26-03: Federal patch by Feb 27, 2026 (48 hours)"	REQUIRED

Note: Mitigation steps reduce exposure but do not eliminate the vulnerability. Patching is the only complete remediation.

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority	Timeframe
Patch Deployment	Apply Cisco security updates	**MANDATORY**	Immediate
Internet Exposure Review	Remove or firewall management interface	**MANDATORY**	Immediate
Account Audit	Review and validate admin accounts	HIGH	Within 24–48 hours
Credential Rotation	Reset credentials and API tokens	HIGH	Within 72 hours
Log Review	Conduct retrospective compromise analysis	REQUIRED	Immediate
Continuous Monitoring	Enable enhanced detection rules	REQUIRED	Ongoing

MONITORING & DETECTION REQUIREMENTS

#	Monitoring Activity
1	Monitor authentication logs for bypass patterns
2	Alert on new administrative account creation
3	Detect unexpected configuration changes
4	Monitor API token creation and privilege escalation
5	Inspect inbound traffic targeting management interface endpoints
6	Correlate SD-WAN logs with SIEM for anomaly detection
7	Review outbound connections from management servers
8	Validate integrity of SD-WAN policy templates

REFERENCES

Reference	URL
Cisco Security Advisory	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHcht2k
NVD Entry	https://nvd.nist.gov/vuln/detail/CVE-2026-27127
CISA Alert	https://www.cisa.gov/news-events/news/immediate-action-required-cisa-issues-emergency-directive-secure-cisco-sd-wan-systems
Talos Blog	https://blog.talosintelligence.com/uat-8616-sd-wan/

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Treat this vulnerability as mission-critical
2	Patch all affected SD-WAN Manager systems immediately
3	Remove public internet exposure of management interfaces
4	Conduct full compromise assessment if exposure existed
5	Rotate all administrative credentials and tokens
6	Monitor continuously for signs of exploitation
7	Validate configuration and policy integrity post-remediation
8	Report confirmed incidents to National CERT immediately

WARNING: Failure to remediate this vulnerability may result in complete network compromise, operational disruption, data exposure, and long-term adversary persistence within enterprise or government infrastructure. Immediate action is required.