Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-20127: UAT-8616 Exploiting Cisco Catalyst SD-WAN Zero-Day

Date of Publication	Admiralty Code	TA Number
February 26, 2026	A1	TA2026057

Summary

First Seen: 2023
Threat Actor: UAT-8616
Affected Products: Cisco Catalyst SD-WAN Controller (formerly SD-WAN vSmart), Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage)
Impact: CVE-2026-20127 is a critical (CVSS 10.0) authentication bypass vulnerability in Cisco Catalyst SD-WAN Controller and Manager that allows unauthenticated remote attackers to impersonate trusted SD-WAN components and gain high-privileged control-plane access. Actively exploited since at least 2023 by the threat actor UAT-8616, the flaw enables rogue peer deployment, network-wide configuration manipulation, and persistent compromise. Adversaries have chained it with CVE-2022-20775 to achieve root access. Immediate patching is required, as no workaround exists and exploitation impacts on-prem, cloud-hosted, and FedRAMP environments.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20127	Cisco Catalyst SD-WAN Controller and Manager Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Controller / SD-WAN Manager	✓	✓	✓
CVE-2022-20775	Cisco SD-WAN Path Traversal Vulnerability	Cisco SD-WAN Software	✗	✓	✓

Vulnerability Details

#1 CVE-2026-20127 is a critical authentication bypass vulnerability (CVSS v3.1 score: 10.0) affecting Cisco Catalyst SD-WAN Controller (formerly vSmart) and Catalyst SD-WAN Manager (formerly vManage). The flaw originates from a fundamental failure in the SD-WAN peering authentication mechanism. The trust validation process responsible for establishing secure control-plane relationships between SD-WAN components does not properly verify identity and credentials, allowing an attacker to introduce a rogue device that is accepted as a legitimate SD-WAN peer. Because the defect is inherent to the authentication logic itself, it is not configuration-dependent and has no workaround.

#2 An unauthenticated remote attacker can exploit the vulnerability by sending specially crafted requests to an exposed controller or manager interface. Successful exploitation grants access as the internal “vmanage-admin” account, a high-privileged non-root user. From there, the attacker can access the NETCONF interface and manipulate configurations across the entire SD-WAN fabric, including routing policies, segmentation rules, and peer relationships. Since the SD-WAN controller governs centralized network orchestration, compromise enables broad control-plane manipulation with high impact to confidentiality, integrity, and availability.

#3 Active exploitation has been confirmed since at least 2023 by the threat actor UAT-8616, targeting global critical infrastructure environments. Observed attack chains show adversaries leveraging CVE-2026-20127 for initial access, then deliberately downgrading the controller software to exploit CVE-2022-20775 (a path traversal privilege-escalation flaw) to obtain root-level access. Attackers subsequently restore the original software version to obscure evidence of compromise. Post-exploitation activity includes unauthorized SSH key deployment, creation and deletion of malicious accounts, log tampering or truncation, rogue control-plane peering events, and persistent backdoor access.

#4 The vulnerability affects multiple SD-WAN releases across on-premises deployments, Cisco Hosted SD-WAN Cloud (including Cisco-managed and FedRAMP environments), and end-of-maintenance versions. Cisco has released fixed software versions and strongly advises immediate upgrades, particularly for unsupported releases. Given its maximum severity rating, lack of workarounds, confirmed zero-day exploitation, and potential for full SD-WAN fabric compromise, CVE-2026-20127 should be treated as a priority-one remediation and threat-hunting event across all affected environments.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20127	Cisco Catalyst SD-WAN Controller & SD-WAN Manager (Before 20.9.8.2, 20.12.6.1, 20.12.5.3, 20.12.6.1, 20.15.4.2, 20.15.4.2, 20.15.4.2, 20.18.2.1, 20.18.2.1)	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:* cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-287
CVE-2022-20775	Cisco SD-WAN Software (Before 20.6.3 to 20.6.4)	cpe:2.3:a:cisco:sd-wan:*:*:*:*:*:*:*:*	CWE-25 CWE-22

Recommendations

Apply Cisco Security Updates Immediately: Upgrade all Cisco Catalyst SD-WAN Controller and SD-WAN Manager instances to the fixed software releases specified by Cisco, including 20.9.8.2, 20.12.5.3, 20.12.6.1, 20.15.4.2, or 20.18.2.1, depending on your current release train. For releases earlier than 20.9 or end-of-life releases such as 20.11, 20.13, 20.14, and 20.16, migrate to a supported fixed release immediately. This is the only complete remediation for CVE-2026-20127, as no workarounds exist.

Conduct Forensic Investigation for Indicators of Compromise: Review the auth.log file located at /var/log/auth.log for entries containing "Accepted publickey for vmanage-admin" from unknown or unauthorized IP addresses. Check for creation or deletion of unfamiliar user accounts, unexpected root sessions, unauthorized SSH keys in /home/vmanage-admin/.ssh/authorized_keys and /home/root/.ssh/authorized_keys, abnormally small or missing log files, evidence of software downgrades and reboots, and unexplained peering events in SD-WAN logs. Validate all control connection peering events against known maintenance windows, authorized IP ranges, and documented device assignments.

Restrict Network Access to SD-WAN Control Components: Implement access control lists (ACLs), security group rules, and firewall rules to restrict traffic to ports 22 and 830 on SD-WAN controllers, allowing only known controller IPs and authorized management hosts. Prevent access from unsecured networks, particularly the internet, to SD-WAN management and control plane interfaces. Deploy controllers behind filtering devices such as firewalls and consider a two-layer firewall architecture to prevent direct end-user access to SD-WAN management infrastructure.

Enable External Log Storage and Enhanced Monitoring: Ensure all SD-WAN system logs are forwarded to external, centralized logging infrastructure such as a SIEM solution to prevent log tampering by a threat actor with root access. Monitor for unexpected traffic patterns, unauthorized peering events, software version changes, and unusual administrative activity. Regularly audit web log traffic for any unexpected traffic to and from SD-WAN systems, and retain logs for a sufficient duration to support post-incident investigation.

Harden SD-WAN Administrative Access: Disable HTTP access to the Cisco Catalyst SD-WAN Manager web UI and use SSL/TLS with certificates from a trusted certificate authority. Change all default administrator passwords to strong, unique alternatives and create role-based user accounts with minimum necessary privileges. Disable any unnecessary network services including HTTP and FTP. Review the Cisco Catalyst SD-WAN Hardening Guide for comprehensive security configuration guidance.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1078: Valid Accounts	
Persistence	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
	T1136: Create Account	
Defense Evasion	T1070: Indicator Removal	T1070.003: Clear Command History
	T1601: Modify System Image	T1601.001: Patch System Image
	T1036: Masquerading	

Tactic	Technique	Sub-technique
Lateral Movement	T1021: Remote Services	T1021.004: SSH
Impact	T1529: System Shutdown/Reboot	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Links

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

https://blog.talosintelligence.com/uat-8616-sd-wan/

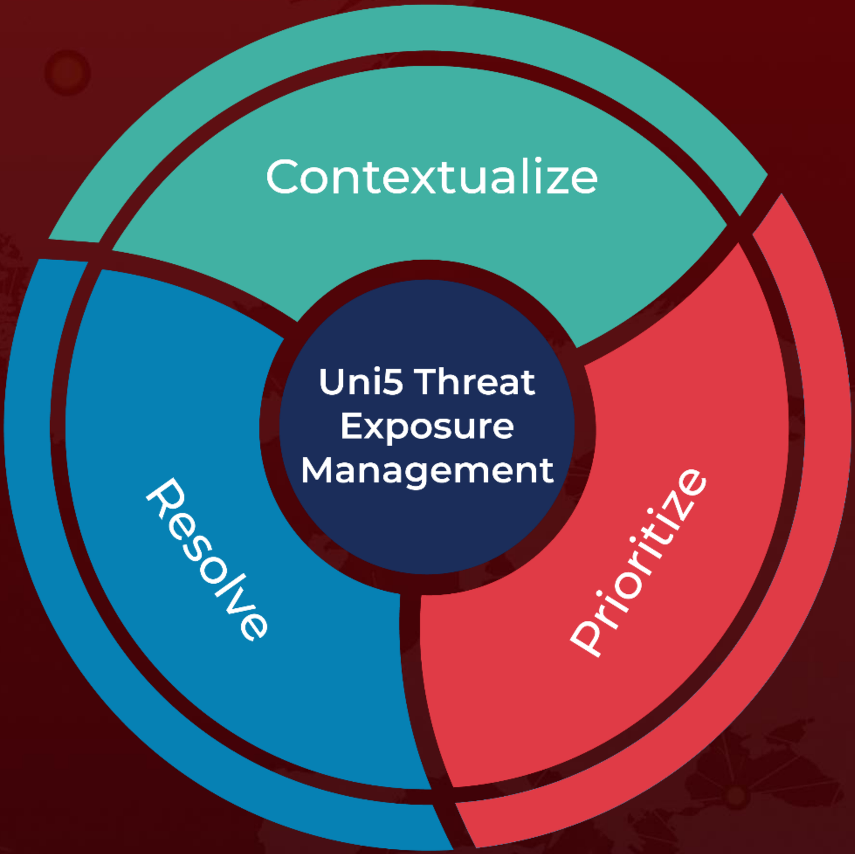
https://www.cisa.gov/news-events/directives/supplemental-direction-ed-26-03-hunt-and-hardening-guidance-cisco-sd-wan-systems

https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 26, 2026 • 10:30 PM

More at www.hivepro.com