Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco SD-WAN Authentication Bypass Exploited in Zero-Day Attacks

Date of Publication	Admiralty Code	TA Number
May 15, 2026	A1	TA2026132

Summary

First Seen: May 2026
Affected Products: Cisco Catalyst SD-WAN Controller (formerly vSmart), Cisco Catalyst SD-WAN Manager (formerly vManage)
Threat Actor: UAT-8616
Impact: Cisco Systems is urging customers to patch a critical zero-day vulnerability in its Catalyst SD-WAN platform after attackers were caught exploiting CVE-2026-20182 to gain root access to exposed systems without valid credentials. The flaw stems from a broken authentication path in the platform's DTLS peering mechanism, allowing threat actors to impersonate trusted devices and silently bypass certificate verification during the handshake process. The vulnerability was exploited by UAT-8616, a sophisticated threat actor associated with Operational Relay Box (ORB) infrastructure. With exploitation requiring little more than a crafted handshake and a self-signed certificate, the vulnerability poses a serious risk to enterprise and SD-WAN deployments worldwide.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20182	Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Controller / Manager	✓	✓	✓

Vulnerability Details

#1

Cisco Systems is warning that a critical authentication bypass vulnerability in its Catalyst SD-WAN Controller platform, tracked as CVE-2026-20182, has been actively exploited as a zero-day, allowing attackers to obtain root privileges on vulnerable devices without valid credentials. This new vulnerability affects the same "vdaemon" service over DTLS (UDP port 12346) that was vulnerable to CVE-2026-20127, but it is not a patch bypass of that earlier flaw; it is a different issue located in a similar part of the vdaemon networking stack. It impacts the peering authentication mechanism within the vdaemon service used by both Cisco Catalyst SD-WAN Controller and SD-WAN Manager. The flaw stems from missing verification logic inside the vbond_proc_challenge_ack() function, which handles CHALLENGE_ACK messages exchanged during the multi-stage DTLS authentication handshake. While the function properly validates certificates for vSmart (type 3), vManage (type 5), and vEdge (type 1) devices, it fails to perform any authentication checks for the vHub device type (type 2). As a result, if a connecting peer identifies itself as a vHub, the request bypasses all validation routines and the peer is automatically marked as authenticated.

#2

The attack can be carried out over the DTLS-over-UDP control-plane peering service running on UDP port 12346, which is used for communication between controllers and edge devices. Exploitation is relatively simple: an attacker initiates a DTLS handshake using any self-signed certificate, receives a CHALLENGE message from the target, and responds with a crafted CHALLENGE_ACK packet where the device_type field is set to 2 (vHub). Because the vulnerable code path skips certificate verification for this device type, authentication succeeds automatically. The attacker can then send a Hello message to move the session into an active “UP” state. The attack does not require valid credentials, trusted certificates, or prior knowledge of the SD-WAN environment. Cisco also noted that the pre-authentication logic in vbond_proc_msg() intentionally allows unauthenticated CHALLENGE_ACK messages to complete the handshake, which inadvertently enables exploitation.

#3

The vulnerability affects all vulnerable Cisco Catalyst SD-WAN deployments regardless of configuration, including on-premises environments, Cisco SD-WAN Cloud-Pro, Cisco Managed SD-WAN Cloud, and FedRAMP-based government deployments. Cisco has released fixes across multiple supported branches, including versions 20.9.9.1, 20.12.5.4, 20.12.6.2, 20.12.7.1, 20.15.4.4, 20.15.5.2, 20.18.2.2, and 26.1.1.1. Older releases such as 20.10, 20.11, 20.13, 20.14, and 20.16 are now end of maintenance, and customers are urged to migrate to supported versions immediately.

#4

Cisco Systems confirmed that CVE-2026-20182 was actively exploited in May 2026, with the activity involving UAT-8616, a sophisticated threat actor that has targeted SD-WAN infrastructure since at least 2023. Researchers also observed overlaps between the group's infrastructure and Operational Relay Box (ORB) networks, which are commonly used to conceal malicious operations and route attacker traffic through compromised devices. The disclosure comes shortly after proof-of-concept exploit code for the related vulnerability chain, CVE-2026-20133, CVE-2026-20128, and CVE-2026-20122, became publicly available in March 2026. Following the release, researchers tracked at least ten separate threat clusters abusing unpatched SD-WAN Manager systems to deploy webshells, backdoors, red-team frameworks, credential stealers, and cryptominers.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20182	Cisco Catalyst SD-WAN before 20.9.9.1, before 20.12.7.1, before 20.12.7.1, before 20.12.5.4, 20.12.6.2, 20.12.7.1, before 20.15.5.2, before 20.15.5.2, before 20.15.4.4, 20.15.5.2, before 20.18.2.2, before 20.18.2.2, before 26.1.1.1	cpe:2.3:a:cisco:catalyst_sd-wan_controller:*:*:*:*:*:*:*:*, cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-287

Recommendations

Apply Cisco Software Updates Immediately: Upgrade all Cisco Catalyst SD-WAN Controller and Manager deployments to the fixed software releases without delay. The specific fixed release depends on the current branch: 20.9.9.1 for the 20.9 branch, 20.12.5.4, 20.12.6.2, or 20.12.7.1 for the 20.12 branch, 20.15.4.4 or 20.15.5.2 for the 20.15 branch, 20.18.2.2 for the 20.18 branch, and 26.1.1.1 for the 26.1.1 branch. Installations running end-of-maintenance releases (20.10, 20.11, 20.13, 20.14, 20.16, or earlier than 20.9) must be migrated to a supported fixed release. There are no workarounds available for this vulnerability.

Conduct Compromise Assessment and Log Review: Audit the /var/log/auth.log file on all SD-WAN controllers for entries showing "Accepted publickey for vmanage-admin" from unknown or unauthorized IP addresses, which is a primary indicator of compromise. Additionally, run the commands "show control connections detail" and "show control connections-history detail" and look for connections with state:up and challenge-ack: 0, which may indicate unauthorized peer connections. Flag any peering events that occur at unexpected times, originate from unrecognized IP addresses, or involve device types inconsistent with the environment's architecture. Check for the presence of unauthorized files such as /cmd.gz/cmd.jsp or suspicious JSP files in deployment directories.

Restrict Network Access to Control Plane Services: Prevent access to the vdaemon DTLS control-plane port (UDP 12346) and the NETCONF service (TCP port 830) from untrusted networks, especially the internet. Place SD-WAN control components behind filtering devices such as firewalls and restrict traffic to known, trusted management hosts only. Disable HTTP for the SD-WAN Manager web UI administrator portal and disable any network services that are not required.

Harden SD-WAN Infrastructure: Change the default administrator password to a strong variant and restrict access to the administrator account by creating user accounts based on necessary access requirements. Create operator accounts for all administrators. Use SSL/TLS with certificates from a certificate authority (CA) or create self-signed certificates. Implement logging to an external server and retain logs for a sufficient duration to support post-event investigations. Review and implement the guidance in the Cisco Catalyst SD-WAN Hardening Guide.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Persistence	T1098: Account Manipulation	T1098.004: SSH Authorized Keys
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

https://www.rapid7.com/blog/post/ve-cve-2026-20182-critical-authentication-bypass-cisco-catalyst-sd-wan-controller-fixed/

https://hivepro.com/threat-advisory/cve-2026-20127-uat-8616-exploiting-cisco-catalyst-sd-wan-zero-day/

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 Demo of **HivePro**.

REPORT GENERATED ON

May 15, 2026 • 10:30 AM

More at www.hivepro.com