Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco Warns of Actively Exploited Flaws in Catalyst SD-WAN Manager

Date of Publication	Admiralty Code	TA Number
March 06, 2026	A1	TA2026063

Summary

First Seen: February 25, 2026
Affected Products: Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage)
Impact: Cisco has disclosed multiple vulnerabilities affecting Cisco Catalyst SD-WAN Manager, warning that two flaws, CVE-2026-20122 and CVE-2026-20128, are already being actively exploited in the wild. The most critical of these allows an authenticated attacker with limited access to overwrite arbitrary files via the API, potentially gaining elevated vManage privileges and altering system behavior. The second exploited issue exposes sensitive credential data associated with the Data Collection Agent (DCA), allowing attackers with valid credentials to retrieve passwords and move laterally across SD-WAN Manager nodes. While several other vulnerabilities were patched as part of the same update, the confirmed real-world exploitation of these two flaws highlights an immediate risk for organizations running affected SD-WAN deployments and underscores the urgency of applying Cisco's security updates.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20122	Cisco Catalyst SD-WAN Manager Arbitrary File Overwrite Vulnerability	Cisco Catalyst SD-WAN Manager	✗	✗	✓
CVE-2026-20128	Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability	Cisco Catalyst SD-WAN Manager	✗	✗	✓
CVE-2026-20129	Cisco Catalyst SD-WAN Manager Authentication Bypass Vulnerability	Cisco Catalyst SD-WAN Manager	✗	✗	✓
CVE-2026-20126	Cisco Catalyst SD-WAN Manager Privilege Escalation Vulnerability	Cisco Catalyst SD-WAN Manager	✗	✗	✓
CVE-2026-20133	Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability	Cisco Catalyst SD-WAN Manager	✗	✗	✓

Vulnerability Details

#1 Cisco has addressed multiple security flaws and disclosed that two vulnerabilities affecting the Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage) are currently being actively exploited in the wild. The issues span a range of impacts, potentially allowing attackers to compromise the SD-WAN management infrastructure if left unpatched.

#2 CVE-2026-20122 is an arbitrary file overwrite vulnerability caused by improper file handling within the API interface. An authenticated remote attacker with valid read-only credentials and API access can upload a malicious file that overwrites arbitrary files on the local file system. By abusing this capability, the attacker can obtain vManage user privileges and potentially manipulate system behavior or introduce malicious components. Cisco confirmed in a March advisory that this vulnerability is actively exploited in real-world attacks.

#3 CVE-2026-20128 is an information disclosure vulnerability affecting the Data Collection Agent (DCA) feature. The issue arises because a credential file associated with the DCA user is stored on the system with insufficient protection. An authenticated local attacker with valid vManage credentials can access the file to obtain the DCA password and then use those credentials to authenticate to other SD-WAN Manager nodes. This could enable lateral movement across the SD-WAN management plane. Cisco has also confirmed that this vulnerability is actively exploited in the wild, highlighting the importance of prompt patching.

#4 CVE-2026-20129 is a critical authentication bypass vulnerability in the API user authentication component. The flaw results from improper authentication handling for API requests, enabling a remote attacker to send a specially crafted API request and bypass authentication controls. Successful exploitation allows the attacker to gain access as a user with the netadmin role.

#5 CVE-2026-20126 is a privilege escalation vulnerability caused by an insufficient authentication mechanism within the REST API. An attacker with low-privileged local access can exploit the flaw by sending a crafted request to the API, ultimately elevating privileges to root on the underlying operating system.

#6 CVE-2026-20133 is an information disclosure vulnerability stemming from insufficient file system access restrictions within the platform. An unauthenticated remote attacker can interact with the system's API to retrieve sensitive data from the underlying operating system. The disclosure comes just a week after Cisco warned that a critical flaw (CVE-2026-20127) affecting Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager was exploited by the sophisticated threat actor UAT-8616 to establish persistent access within high-value organizations.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20122	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-648
CVE-2026-20128	Cisco Catalyst SD-WAN Manager (Before 20.18)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-257
CVE-2026-20129	Cisco Catalyst SD-WAN Manager (Before 20.18)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-287
CVE-2026-20126	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-648
CVE-2026-20133	Cisco Catalyst SD-WAN Manager (Before 20.9.8.2 / 20.12.6.1 / 20.15.4.2 / 20.18.2.1)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*	CWE-200

Recommendations

Upgrade to Fixed Software Immediately: Organizations running Cisco Catalyst SD-WAN Manager must prioritize upgrading to the fixed releases identified in Cisco's advisory. The recommended fixed versions are 20.9.8.2 for the 20.9 release train, 20.12.5.3 or 20.12.6.1 for the 20.12 train, 20.15.4.2 for releases 20.13 through 20.15, and 20.18.2.1 for releases 20.16 and 20.18. Active exploitation of CVE-2026-20128 and CVE-2026-20122 makes this upgrade critically time-sensitive, and organizations should treat this as an emergency patching activity. Consult the Cisco Catalyst SD-WAN Upgrade Matrix for planning guidance.

Restrict Network Access to the Management Plane: Prevent access to Cisco Catalyst SD-WAN Manager from unsecured networks, especially the internet. Deploy the SD-WAN management platform behind a filtering device such as a firewall and restrict access to known, trusted hosts only. A two-layer firewall architecture is recommended to ensure that end users do not connect directly to the outer DMZ, reducing the API attack surface for the unauthenticated vulnerabilities (CVE-2026-20129 and CVE-2026-20133).

Conduct Compromise Assessment and Credential Rotation: Given confirmed in-the-wild exploitation, organizations should perform a thorough compromise assessment of their SD-WAN Manager infrastructure. Review all user accounts for unauthorized additions, inspect logs for anomalous API activity, and check for unexpected file modifications. Rotate all credentials associated with the SD-WAN Manager platform, including the default administrator password, vmanage user credentials, and DCA user passwords, as CVE-2026-20128 directly exposes stored DCA credentials.

Disable Unnecessary Network Services: Disable HTTP access for the Cisco Catalyst SD-WAN Manager web UI administrator portal and any other network services that are not operationally required, including HTTP and FTP. Reducing the service footprint limits the available attack surface, particularly for API-based exploitation vectors. Ensure SSL/TLS is enforced for all remaining management communications using certificates obtained from a trusted certificate authority.

Implement Enhanced Monitoring and Logging: Establish continuous monitoring of API traffic to and from the SD-WAN Manager nodes, with alerts configured for unusual authentication patterns, file system modifications, and privilege escalation indicators. Logging should be forwarded to an external SIEM or syslog server to prevent log tampering by an attacker with root access. Retain logs for a sufficient duration to support post-incident forensic analysis.

Review End-of-Life Release Exposure: Multiple affected Cisco Catalyst SD-WAN Manager release trains have reached End of Software Maintenance. Organizations running these releases should plan immediate migration to a supported release, as they will not receive future security updates. Continued operation on end-of-life software exposes the organization to cumulative risk from both current and future vulnerabilities.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Credential Access	T1552: Unsecured Credentials	T1552.001: Credentials In Files
Lateral Movement	T1021: Remote Services	
Impact	T1565: Data Manipulation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

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

References

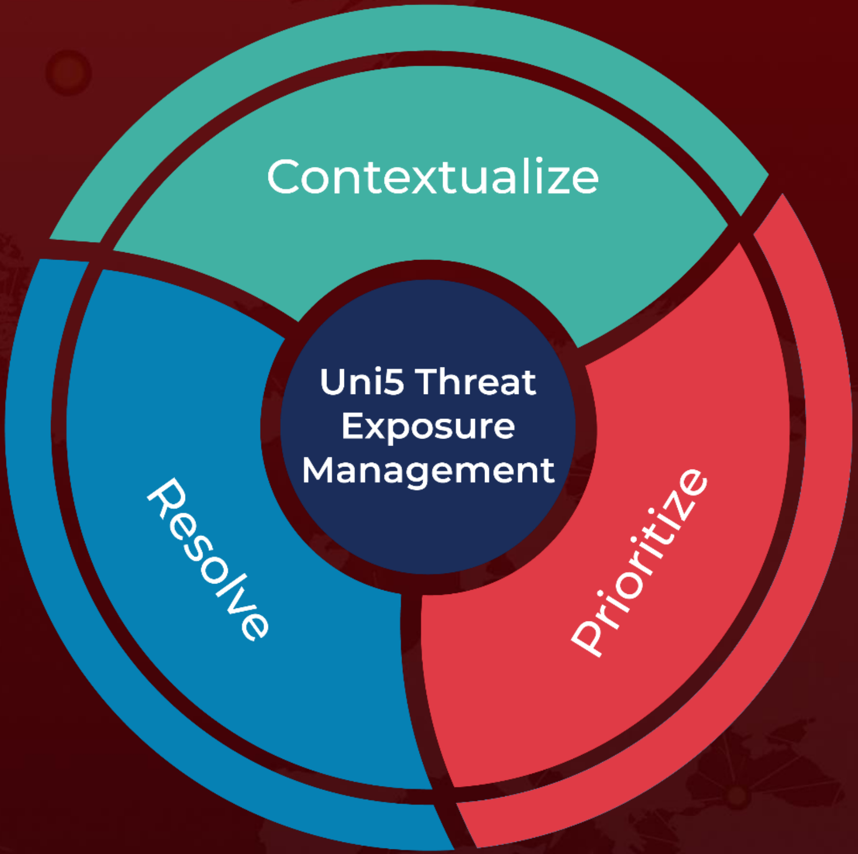
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

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



REPORT GENERATED ON

March 06, 2026 • 5:50 AM

More at www.hivepro.com