Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Cisco SD-WAN Under Fire: Exploited Path Traversal Bug Enables Root-Level Access

Date of Publication	Admiralty Code	TA Number
June 16, 2026	A1	TA2026168

Summary

First Seen: June 2026 (exploitation telemetry in Cisco's published log samples is dated June 11, 2026)
Affected Products: Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage)
Impact: Cisco Catalyst SD-WAN Manager is affected by CVE-2026-20262. This critical path traversal vulnerability allows remote attackers to write arbitrary files on the underlying operating system through a crafted file upload request. The flaw can be leveraged to overwrite existing files or create new ones, potentially paving the way for privilege escalation to root and complete appliance compromise. Affecting all deployment models and multiple software versions, the vulnerability is particularly concerning as Cisco has confirmed active exploitation, underscoring the urgency for organizations to apply available security updates.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-20262	Cisco Catalyst SD-WAN Manager Directory or Path Traversal Vulnerability	Cisco Catalyst SD-WAN Manager	✓	✓	✓

Vulnerability Details

#1

CVE-2026-20262 is a critical arbitrary file write vulnerability affecting the web-based management interface of Cisco Catalyst SD-WAN Manager, formerly known as SD-WAN vManage. Tracked under CWE-22 (Path Traversal), the flaw stems from improper validation of user-supplied input during the file upload process. As a result, an attacker can manipulate file paths and bypass intended directory restrictions, allowing unauthorized file operations on the underlying system.

#2

The vulnerability originates from insufficient input sanitization within a file upload functionality exposed through an affected API endpoint. By sending a specially crafted HTTP request, a remote attacker can exploit the path traversal weakness to write files outside the designated upload directory. This enables the creation of new files or the overwriting of existing ones anywhere on the operating system, significantly increasing the potential impact of the attack.

#3

According to Cisco, the arbitrary file write capability can serve as a steppingstone for further compromise. A maliciously written file could be leveraged to escalate privileges to root, giving an attacker complete administrative control over the appliance. This transforms the vulnerability from a simple file manipulation issue into a potential pathway for full system takeover.

#4

The flaw affects Cisco Catalyst SD-WAN Manager across all deployment models, including on-premises environments, Cisco SD-WAN Cloud-Pro, Cisco SD-WAN Cloud (Cisco Managed), and Cisco SD-WAN for Government (FedRAMP). Vulnerable versions span multiple software release trains through 26.1.x series. Cisco has confirmed that the vulnerability was actively exploited in limited attacks observed in June 2026, although no specific threat actor or malware campaign has been publicly linked to the activity.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-20262	Cisco Catalyst SD-WAN Manager (releases 20.9.9.1 and earlier, 20.12.7.1 and earlier, 20.15.4.4 and earlier, 20.15.5.2 and earlier, 20.18.3, and 26.1.1.1 and earlier)	cpe:2.3:a:cisco:catalyst_sd-wan_manager:*:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Apply the Cisco Fixed Software Immediately: Upgrade Cisco Catalyst SD-WAN Manager to the first fixed release for your train without delay, 20.9.9.2, 20.12.7.2, 20.15.4.5, 20.15.5.3, 20.18.3.1, or 26.1.1.2 as applicable. Cisco has confirmed this vulnerability is being exploited in the wild, has added it to mandatory remediation tracking, and has stated there are no workarounds, so patching is the only effective remediation.

Restrict Management-Plane Exposure: Ensure SD-WAN Manager is not reachable from the public internet. Because exploitation requires a valid low-privilege account and a reachable API endpoint, limiting network exposure to trusted management networks and enforcing strict access controls materially reduces the attack surface even before patching completes.

Review and Harden Account Access: Audit all SD-WAN Manager user accounts, including lower-privileged and single-task accounts, since the vulnerability is exploitable by exactly these account types. Remove unused or unrecognized accounts, rotate credentials where compromise is suspected, and enforce strong authentication and least-privilege practices for all management-plane access.

Hunt for Indicators of Compromise: Review the SD-WAN Manager log files for signs of exploitation published by Cisco. Audit vmanage-server.log and vmanage-appserver.log (under /var/log/nms) for unexpected file uploads or WAR deployments into the WildFly standalone deployments directory, and review serviceproxy-access.log (under /var/log/nms/containers/service-proxy/) for HTTP POST requests to unrecognized JSP endpoints. If suspicious entries are found, open a case with the Cisco Technical Assistance Center (TAC) and provide a request admin-tech output for review.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
Persistence	T1505: Server Software Component	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Details

Upgrade Cisco Catalyst SD-WAN Manager to the latest fixed release: 20.9.9.2, 20.12.7.2, 20.15.4.5, 20.15.5.3, 20.18.3.1, 26.1.1.2.

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

References

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-arbfw-c2rZvQ

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

June 16, 2026 • 08:45 AM

More at www.hivepro.com