

CVE-2026-20245

Cisco Catalyst SD-WAN Manager Improper Encoding or Escaping of Output Vulnerability

CISA KEV since Jun 9, 2026

Actively exploited

A vulnerability in the CLI of Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond, could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by uploading a crafted file to the affected system.

EVRS 75 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.253 97.9th percentile · FIRST	CISA DEADLINE Jun 23, 2026 CISA federal deadline · Overdue by 4 months
---	--	--	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last year
☒ EPSS	0.253 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

A successful exploit could allow the attacker to perform command injection attacks on an affected system and elevate their privileges as the root user. To exploit this vulnerability, the attacker must have netadmin privileges on the affected system. This would require valid credentials or exploitation of or . Cisco is not aware of successful exploitation by other methods. Cisco has observed limited cases where the exploitation of this bug resulted in a configuration change pushed to edge devices. Cisco recommends that customers upgrade to the fixed software that is documented in the that was published on May 14, 2026, and verify the configuration of the edge devices.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
catalyst sd-wan manager	< 20.9.9.1	no fixed version listed	NVD
	≥ 20.10 < 20.12.5.4		
	≥ 20.12.6 < 20.12.6.2		
	≥ 20.13 < 20.15.4.4		
	≥ 20.15.5 < 20.15.5.2		
	≥ 20.16 < 20.18.2.2		
	≥ 26.1 < 26.1.1.1		
	20.12.7		
sd-wan vsmart controller	< 20.9.9.1	no fixed version listed	NVD
	≥ 20.10 < 20.12.5.4		
	≥ 20.12.6 < 20.12.6.2		
	≥ 20.13 < 20.15.4.4		
	≥ 20.15.5 < 20.15.5.2		
	≥ 20.16 < 20.18.2.2		
	≥ 26.1 < 26.1.1.1		
	20.12.7		

Sources

Vendor guidance	github.com/advisories/GHSA-h4c6-cm2m-h5f6	Additional guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
NVD	nvd.nist.gov/vuln/detail/CVE-2026-20245	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-34341	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-20245

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.