

CVE-2022-20775

Cisco SD-WAN Path Traversal Vulnerability

CISA KEV since Feb 25, 2026

Actively exploited

A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges. This vulnerability is due to improper access controls on commands within the application CLI. An attacker could exploit this vulnerability by running a maliciously crafted command on the application CLI. A successful exploit could allow the attacker to execute arbitrary commands as the root user. Cisco has released software updates that address this vulnerability.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.125 96.2nd percentile · FIRST	CISA DEADLINE Feb 27, 2026 CISA federal deadline · Overdue by 8 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	0.125 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: Please adhere to CISA's guidelines to assess exposure and mitigate risks associated with Cisco SD-WAN devices as outlines in CISA's Emergency Directive 26-03 (URL listed below in Notes) and CISA's "Hunt & Hardening Guidance for Cisco SD-WAN Devices (URL listed below in Notes). Adhere to the applicable BOD 22-01 guidance for cloud services or discontinue use of the product if mitigations are not available.
Basis: CISA KEV required action

There are no workarounds that address this vulnerability. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF>

Affected and fixed versions · 76 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
catalyst sd-wan manager	< 20.6.3 ≥ 20.7 < 20.7.2 20.8	20.6.3 · 20.7.2	NVD
sd-wan vbond orchestrator	< 20.6.3 ≥ 20.7 < 20.7.2 20.8	20.6.3 · 20.7.2	NVD
sd-wan vedge cloud	< 20.6.3 ≥ 20.7 < 20.7.2 20.8	20.6.3 · 20.7.2	NVD
sd-wan vsmart controller	< 20.6.3 ≥ 20.7 < 20.7.2 20.8	no fixed version listed	NVD
sd-wan	< 20.6.3 ≥ 20.7 < 20.7.2 20.8	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
catalyst 8000v edge	–	no fixed version listed	NVD
catalyst cg418-e	–	no fixed version listed	NVD
catalyst cg522-e	–	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-x65r-rvgh-v43v	Additional guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF
CISA Mitigation Instructions	cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems	cisa.gov	cisa.gov/news-events/directives/supplemental-direction-ed-26-03-hunt-and-hardening-guidance-cisco-sd-wan-systems
cisco.com	cisco.com/c/en/us/support/docs/csa/cisco-sa-sd-wan-priv-E6e8tEdF.html	NVD	nvd.nist.gov/vuln/detail/CVE-2022-20775
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2022-26025
Current data	evulnable.com/vulnerability-management/cve/CVE-2022-20775		

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