

CVE-2026-20182

Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

Exigent

CISA KEV since May 14, 2026

Actively exploited

Public exploit module (Metasploit)

May 2026: This security advisory provides the details and fix information for a vulnerability that was discovered and fixed after the was disclosed in February 2026. This new advisory is for a new vulnerability in the control connection handshaking. The section of this advisory includes Show Control Connections guidance to help with system checks. A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage,

EVRS 88/100 Immediate priority	CVSS V3.1 10.0 Critical · NVD	EPSS 0.918 99.82nd percentile · FIRST	CISA DEADLINE May 17, 2026 CISA federal deadline · Overdue by 5 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	0.918 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 10.0	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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 outlined 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

and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system. This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to the affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
catalyst sd-wan manager	< 20.9.9.1 ≥ 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	no fixed version listed	NVD
sd-wan vbond orchestrator	< 20.9.9.1 ≥ 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	no fixed version listed	NVD
sd-wan vsmart controller	< 20.9.9.1 ≥ 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	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p83j-mxpw-gqpj	Additional guidance	sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
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
NVD	nvd.nist.gov/vuln/detail/CVE-2026-20182	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2026-30324	Current data	evulnable.com/vulnerability-management/cve/CVE-2026-20182

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