Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-20182
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 17:16:19 UTC
Updated	2026-05-15 12:45:53 UTC
Description	May 2026: This security advisory provides the details and fix information for a vulnerability that was discovered and fixed af

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from psirt@cisco.com

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

EPSS: 0.379540000 probability, percentile 0.972630000 (date 2026-05-16)

CISA KEV: Listed on 2026-05-14; due 2026-05-17; ransomware use Unknown

Problem Types: CWE-287 | CWE-287 Improper Authentication

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Secondary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSSV3_1	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	Catalyst SD-WAN
Name	Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability
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.
Notes	CISA Mitigation Instructions: https://www.cisa.gov/news-events/directives/ed-26-03-mitigate-vulnerabilities-cisco-sd-wan-systems ; https://www.cisa.gov/news-events/directives/supplemental-direction-ed-26-03-hunt-and-hardening-guidance-cisco-sd-wan-systems ; https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW ; https://nvd.nist.gov/vuln/detail/CVE-2026-20182

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Catalyst Sd-wan Manager	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.12	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.099	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.7	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.1.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.303	Not specified

CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.098	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.6.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.2.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.8	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.3.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.9	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.501_ES	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.929	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.31	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.4.0.9	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.3.1	Not specified

References

Reference	Source	Link
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0	www
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-...	psirt@cisco.com	sec.
sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-...	psirt@cisco.com	sec.
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.
CISA Known Exploited Vulnerabilities catalog	CISA	www

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event

ADP	2026-05-14T00:00:00.000Z	CVE-2026-20182 added to CISA KEV

Exploits

CNA: In May 2026, the Cisco Product Security Incident Response Team (PSIRT) became aware of limited exploitation of this vulnerability. Cisco strongly recommends that customers upgrade to a fixed software release to remediate this vulnerability.

There are currently no legacy QID mappings associated with this CVE.