Cisco Catalyst SD-WAN Manager Information Disclosure Vulnerability

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

Summary

CVE	CVE-2026-20128
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-25 17:25:30 UTC
Updated	2026-04-21 12:48:20 UTC
Description	A vulnerability in the Data Collection Agent (DCA) feature of Cisco Catalyst SD-WAN Manager could allow an unauthentica

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from psirt@cisco.com

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

EPSS: 0.000620000 probability, percentile 0.192790000 (date 2026-04-21)

CISA KEV: Listed on 2026-04-20; due 2026-04-23; ransomware use Unknown

Problem Types: CWE-257 | CWE-257 Storing Passwords in a Recoverable Format

Version	Source	Type	Score	Severity	Vector
3.1	psirt@cisco.com	Secondary	7.5	HIGH	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H
3.1	CNA	CVSSV3_1	7.5	HIGH	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Changed

Confidentiality

Confidentiality

High

Integrity

High

Availability

High

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

CISA Known Exploited Vulnerability

Vendor	Cisco
Product	Catalyst SD-WAN Manager
Name	Cisco Catalyst SD-WAN Manager Storing Passwords in a Recoverable Format Vulnerability
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.
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-authbp-qwCX8D4v ; https://nvd.nist.gov/vuln/detail/CVE-2026-20128

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 19.3.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.2	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 18.3.8	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.0.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.1.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.302	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.303	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.097	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.098	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.10	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.6.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.0.1a	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.2.0	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.1	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 18.3.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 17.2.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.3.5	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 17.2.7	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 20.3.1	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 19.2.32	Not specified

CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2.1_927	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 18.4.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2_928	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2_929	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.1.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2.1_930	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.5.0.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.4.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2_937	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.5.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.1.1.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.1.0.02	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.1.7	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.1.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.5.1.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.1.10	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.8	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.14	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 19.2.4.0.8	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 20.3.4.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2.0.5	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.5.1.0.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.1.1	Not specified

CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.0.18.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.2.0.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.0.18.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.0.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.16	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.1.0.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.7.1EFT2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.9	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.11	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.0.18	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.1.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.813	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.19	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.5.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.814	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.2.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.20	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.2.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.2.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.0.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.24	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.2.7	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.2.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.2.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.5.0.8	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.5.0.9	Not specified

CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.5.0.7	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.3.0.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.9.1EFT2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.6	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.7	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.4.2.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.5.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.3	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.3.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.7.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.4.0.25	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.2.2.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.1.2	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.1.3.1	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.6.5.1.4	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.3.8	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 20.12.501	Not specified
CNA	Cisco	Cisco Catalyst SD-WAN Manager	affected 26.1.1	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.
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	2026-04-20T00:00:00.000Z	CVE-2026-20128 added to CISA KEV

Exploits

CNA: The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities that are described in CVE-2026-20133, CVE-2026-20126, and CVE-2026-20129. In March 2026, the Cisco PSIRT became aware of active exploitation of the

vulnerabilities that are described in CVE-2026-20128 and CVE-2026-20122 only. The vulnerabilities that are described in the other CVEs in this advisory are not known to have been compromised. Cisco strongly recommends that customers upgrade to a fixed software release to remediate these vulnerabilities.

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