An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2602260203

NCSC Advisory

Critical Vulnerabilities in Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager

26th, February 2026

STATUS: TLP:CLEAR

Description

Cisco have release a number of advisories related to critical vulnerabilities in Cisco Catalyst SD-WAN.

The full list of CVE's is CVE-2026-20127, CVE-2026-20129, CVE-2026-20126, CVE-2026-20133, CVE-2026-20122, CVE-2026-20128. Please review the Cisco advisories page for more details:
https://sec.cloudapps.cisco.com/security/center/publicationListing.x

CVE ID: CVE-2026-20127

Published: 2026-02-25

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Controller (Formerly Cisco Catalyst SD-WAN Manager)

CVSS Score[1]: 10

CVE ID: CVE-2026-20129

Published: 2026-02-25

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Manager

CVSS Score: 9.8

CVE ID: CVE-2026-20128

Published: 2026-02-25

Vendor: Cisco

Product: Cisco Catalyst SD-WAN Manager

CVSS Score: 7.5

[1] https://www.first.org/cvss/

Products Affected

These vulnerabilities affect Cisco Catalyst SD-WAN Manager, regardless of device configuration. A table of fixed releases is shown below, please see Cisco Advisories[2] for full list of impacted versions.

Cisco Catalyst SD-WAN Manager Release	First Fixed Release
Earlier than 20.91	Migrate to a fixed release.
20.9	20.9.8.2 (Estimated release February 27, 2026)
20.111	20.12.6.1
20.12.5 20.12.6	20.12.5.3 20.12.6.1
20.131	20.15.4.2
20.141	20.15.4.2
20.15	20.15.4.2
20.161	20.18.2.1
20.18	20.18.2.1

Impact

A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system.

Malicious cyber threat actors are targeting SD-WANs of organisations globally. After exploitation of this vulnerability the malicious actors add a rogue peer and eventually gain root access to establish long-term persistence in SD-WANs.

[2] https://sec.cloudapps.cisco.com/security/center/publicationListing.x

CVE ID: CVE-2026-20127

- **Common Weakness Enumeration (CWE)[3]:** CWE-287: Improper Authentication
- **Known Exploited Vulnerability (KEV) catalog[4]**: Yes
- **Used by Ransomware Operators**: N/A

CVE ID: CVE-2026-20129

- **Common Weakness Enumeration (CWE):** CWE-287: Improper Authentication
- **Known Exploited Vulnerability (KEV) catalog**: No
- **Used by Ransomware Operators**: N/A

CVE ID: CVE-2026-20128

- **Common Weakness Enumeration (CWE):** CWE-257: Storing Passwords in a Recoverable Format
- **Known Exploited Vulnerability (KEV) catalog:** No
- **Used by Ransomware Operators**: N/A

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority. Affected organisations should review the latest release notes and install the relevant updates from Cisco.

A number of agencies have released a Cisco SD-WAN Threat Hunt Guide (the "Hunt Guide"), based on investigative data, to support network defenders' detection of and response to the malicious actors' threat activity. This can be found in the Further Resources section below.

Some practical steps shared by CISA[5] include:

- Inventory all in-scope Cisco SD-WAN systems,
- Collect artifacts, including virtual snapshots and logs off of SD-WAN systems to support threat hunt activities,

[3] https://cwe.mitre.org

[4] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[5] https://www.cisa.gov/news-events/alerts/2026/02/25/cisa-and-partners-release-guidance-ongoing-global-exploitation-cisco-sd-wan-systems

- Fully patch Cisco SD-WAN systems with available updates,
- Hunt for evidence of compromise, and
- Concurrently review Cisco's latest security advisories, Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability and Cisco Catalyst SD-WAN Vulnerabilities, and implement Cisco's SD-WAN Hardening Guidance

As a temporary measure, Cisco recommends restricting access to port 22 and port 830 via ACLs or firewall rules to known controller IPs. Management interfaces should not be accessible from the Internet.

Further Resources

- https://www.ncsc.gov.uk/news/exploitation-cisco-catalyst-sd-wans
- Hardening Guide: https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide
- Hunt guide: https://www.cyber.gov.au/sites/default/files/2026-02/ACSC-led Cisco SD-WAN Hunt Guide.pdf
- Cisco Catalyst SD-WAN Vulnerabilities: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
- Cisco Catalyst SD-WAN Controller Vulnerability: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-20127
- https://nvd.nist.gov/vuln/detail/CVE-2026-20127
- https://nvd.nist.gov/vuln/detail/CVE-2026-20129
- https://nvd.nist.gov/vuln/detail/CVE-2026-20128