CERT-EU

Security Advisory 2026-002

Multiple Vulnerabilities in Cisco Products

2026-02-25 — v1.0

TLP:CLEAR

History:

- *25/02/2026 — v1.0 – Initial publication*

Summary

On 25 February 2026, Cisco released security advisories addressing multiple high and critical severity vulnerabilities in Cisco Catalyst SD-WAN controllers and Cisco SD-WAN Manager [1,2]. If exploited, these vulnerabilities could allow attackers to gain administrative access to compromised systems.

It is recommended to capture forensic evidence, hunt for indicators of compromise, and apply updates as soon as possible.

One of the vulnerabilities, **CVE-2026-20127**, is **exploited in the wild** since 2023. [4]

Technical Details

Vulnerabilities Affecting Cisco Catalyst SD-WAN Controller

The vulnerability **CVE-2026-20127**, with the CVSS score of 10, is an **authentication bypass vulnerability** in **Cisco Catalyst SD-WAN Controller**, formerly **SD-WAN vManager**. Successful exploitation allows a remote, unauthenticated attacker to obtain administrative privileges on the device. [1]

An attacker could then modify configurations, add rogue devices to the SD-WAN fabric, extract sensitive configuration data, or establish persistent access. [1]

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 an 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. [1]

Vulnerabilities Affecting Cisco Catalyst SD-WAN Manager

Multiple vulnerabilities in **Cisco Catalyst SD-WAN Manager**, formerly **SD-WAN vManage**, could allow an attacker to access an affected system, elevate privileges to root, gain access

to sensitive information, and overwrite arbitrary files. [2]

The vulnerabilities are not dependent on one another. Exploitation of one of the vulnerabilities is not required to exploit another vulnerability.

The vulnerability **CVE-2026-20129**, with a CVSS score of 9.8, is an **authentication bypass vulnerability** in the API user authentication of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to gain access to an affected system as a user who has the *netadmin* role. [2]

The vulnerability **CVE-2026-20126**, with a CVSS score of 7.8, is a **privilege escalation vulnerability** which could allow an authenticated, local attacker with low privileges to gain root privileges on the underlying operating system. This vulnerability is due to an insufficient user authentication mechanism in the REST API. An attacker could exploit this vulnerability by sending a request to the REST API of the affected system. A successful exploit could allow the attacker to gain *root* privileges on the underlying operating system. [2]

The vulnerability **CVE-2026-20133**, with a CVSS score of 7.5, is an **information disclosure vulnerability** which could allow an unauthenticated, remote attacker to view sensitive information on an affected system. This vulnerability is due to insufficient file system access restrictions. An attacker could exploit this vulnerability by accessing the API of an affected system. [2]

The vulnerability **CVE-2026-20122**, with a CVSS score of 7.1, is an **arbitrary file overwrite vulnerability** in the API which could allow an authenticated, remote attacker to overwrite arbitrary files on the local file system. To exploit this vulnerability, the attacker must have valid read-only credentials with API access on the affected system. This vulnerability is due to improper file handling on the API interface of an affected system. An attacker could exploit this vulnerability by uploading a malicious file on the local file system. A successful exploit could allow the attacker to overwrite arbitrary files on the affected system and gain vmanage user privileges. [2]

The vulnerability **CVE-2026-20128**, with a CVSS score of 5.5, is an **information disclosure vulnerability** in the Data Collection Agent (DCA) feature which could allow an authenticated, local attacker to gain DCA user privileges on an affected system. To exploit this vulnerability, the attacker must have valid vmanage credentials on the affected system. This vulnerability is due to the presence of a credential file for the DCA user on an affected system. An attacker could exploit this vulnerability by accessing the file system as a low-privileged user and reading the file that contains the DCA password from that affected system. [2]

Affected Products

The following versions of the Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager are affected:

- all versions earlier than 20.9 (end of software maintenance);
- all versions 20.9 up until 20.9.8.2;
- all versions 20.11 (end of software maintenance);
- all versions 20.12.5 up until 20.12.5.3;
- all versions 20.12.6 up until 20.12.6.1;
- all versions 20.13 (end of software maintenance);
- all versions 20.14 (end of software maintenance);
- all versions 20.15 up until 20.15.4.2;
- all versions 20.16 (end of software maintenance);
- all versions 20.18 up until 20.18.2.1.

Organisations are encouraged to consult the Cisco Catalyst SD-WAN Upgrade Matrix.

Recommendations

CERT-EU recommends the following immediate actions:

- Securing forensic evidence to detect any signs of exploitation as well as reviewing SD-WAN configuration to find any unauthorised changes, following the hunting guide. [4]
- Update affected devices to the appropriate fixed latest version of Cisco Catalyst SD-WAN Manager and Cisco Catalyst SD-WAN Controller as detailed in their respective advisories. [1,2]
- Identify and restrict external access to SD-WAN management (HTTPS, SSH, API) and control plane interfaces. Remove direct internet exposure and limit access to dedicated management networks by following Cisco's hardening guide. [6]

The hunting guide [4] further notes that, in observed exploitation cases, threat actors downgraded SD-WAN Manager to a software version vulnerable to **CVE-2022-20775** in order to facilitate privilege escalation and establish persistence by creating local accounts. [3,4]

If a compromise is suspected, and after ensuring that forensic evidence is secured, contact the relevant cybersecurity authority.

Indicators of Compromise

Organisations are encouraged perform the following checks to identify possible exploitation of the vulnerability **CVE-2026-20127**:

- Audit authentication logs in the auth.log file, located at /var/log/auth.log, for entries that are related to Accepted publickey for *vmanage-admin* from unknown or unauthorised IP addresses, as shown in the following example:

```
2026-02-10T22:51:36+00:00 vm  sshd[804]: Accepted publickey for vmanage-admin from  port
  [REDACTED PORT] ssh2: RSA SHA256:[REDACTED KEY]
```

- Validate peering events against the following checklist:
  - Verify the timestamp of each peering event against known maintenance windows, scheduled configuration changes, and normal operational hours.
  - Confirm the public IP address corresponds to infrastructure owned or operated by authorised organisation or partners by cross-referencing against asset inventories and authorised IP ranges.
  - Validate that the peer system IP matches documented device assignments within the SD-WAN topology.
  - Review the peer type (vmanage, vsmart, vedge, vbond) to ensure it aligns with expected device roles in the related deployment.
  - Correlate multiple events from the same source IP or system IP to identify patterns of reconnaissance or persistent access attempts.
  - Cross-reference event timing with authentication logs, change management records, and user activity to establish whether the connection was initiated by authorised personnel.

```
Jul 26 22:03:33 vSmart-01 VDAEMON_0[2571]: %Viptela-vSmart-VDAEMON_0-5-NTCE-1000001: control-
  connection-state-change new-state:up peer-type:vmanagepeer-system-ip:[PRIVATE IP] public-
```

```
ip:[PUBLIC IP] public-port:[PUBLIC PORT] domain-id:1 site-id:1005
```

More information and indicators of compromise are available in the hunting guide. [4]

References

[1] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk

[2] https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v

[3] https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-sd-wan-priv-E6e8tEdF.html

[4] https://www.cyber.gov.au/sites/default/files/2026-02/ACSC-led%20Cisco%20SD-WAN%20Hunt%20Guide.pdf

[5] https://www.ncsc.gov.uk/news/exploitation-cisco-catalyst-sd-wans

[6] https://sec.cloudapps.cisco.com/security/center/resources/Cisco-Catalyst-SD-WAN-HardeningGuide