مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerabilities in Cisco Catalyst SD-WAN Manager

Tracking #:432318816

Date:21-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple high-severity vulnerabilities in Cisco Catalyst SD-WAN Manager. These flaws are actively being exploited in the wild and could allow attackers to gain unauthorized access, overwrite critical system files, and expose sensitive data.

TECHNICAL DETAILS:

Vulnerability Details
High-Severity Vulnerabilities
CVE-2026-20122 – Arbitrary File Overwrite

- A flaw in the API allows an authenticated attacker with read-only credentials to upload malicious files and overwrite arbitrary files on the system. Successful exploitation can lead to privilege escalation and potential system compromise.

CVE-2026-20128 – Information Disclosure (DCA Credentials)

- An unauthenticated attacker can retrieve sensitive credential files related to the Data Collection Agent (DCA). This may allow attackers to gain DCA user privileges and pivot to other systems.

CVE-2026-20133 – Information Disclosure

- Due to insufficient file system restrictions, attackers can access sensitive information via exposed APIs, potentially revealing critical system-level data.

Affected Products

- Cisco Catalyst SD-WAN Manager

Fixed Versions

- Versions earlier than 20.9: Upgrade to a supported fixed release.
- Version 20.9: Upgrade to 20.9.8.2.
- Versions 20.10 and 20.11: Upgrade to 20.12.6.1.
- Version 20.12: Upgrade to 20.12.5.3 or 20.12.6.1.
- Versions 20.13, 20.14, and 20.15: Upgrade to 20.15.4.2.
- Versions 20.16 and 20.18: Upgrade to 20.18.2.1.

Note: Refer to the official Cisco advisory for indicators of compromise and additional information.

RECOMMENDATIONS:

- Upgrade to the latest fixed version immediately.
- Restrict access to trusted networks and hosts only.
- Use firewalls and monitor logs for suspicious activity.
- Disable unnecessary services (e.g., HTTP/FTP) and enforce SSL/TLS.
- Strengthen authentication (change default passwords, use role-based access).

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
- https://nvd.nist.gov/vuln/detail/CVE-2026-20133