مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Actively Exploited Vulnerability in Cisco Catalyst SD-WAN Manager

Tracking #:432319140

Date:16-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Cisco Catalyst SD-WAN Manager (formerly vManage) is being actively exploited in the wild. The flaw allows an authenticated remote attacker to create or overwrite arbitrary files on the underlying operating system, potentially leading to privilege escalation and full compromise of the SD-WAN management platform.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-20262**
  Severity: Medium | CVSS: 6.5
- The vulnerability exists in the web-based management interface of Cisco Catalyst SD-WAN Manager due to insufficient validation of user-supplied input during file upload operations. An authenticated attacker with valid credentials, including low-privileged accounts, can send crafted HTTP requests to vulnerable API endpoints to create or overwrite files on the system.
- Cisco has stated that the uploaded files may subsequently be leveraged to gain root-level privileges, increasing the impact of the vulnerability.
- Cisco has confirmed limited exploitation of CVE-2026-20262 in the wild as of June 2026.

Affected Products and Versions

Cisco Catalyst SD-WAN Manager, regardless of device configuration
All deployment models are affected, including:

- On-Prem Deployment
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud (Cisco Managed)
- Cisco SD-WAN for Government (FedRAMP)

Cisco Catalyst SD-WAN Release:

- 20.9.9.1 and earlier
- 20.12.7.1 and earlier
- 20.15.4.4 and earlier
- 20.15.5.2 and earlier
- 20.18.3
- 26.1.1.1 and earlier

Fixed Versions

- 20.9.9.2
- 20.12.7.2
- 20.15.4.5
- 20.15.5.3
- 20.18.3.1
- 26.1.1.2

Indicators of Compromise (IoCs)

- Upload and deployment of a suspicious file named **"suspicious.war"**
- Requests to unauthorized or unexpected web pages deployed within the vManage environment

- Unusual activity in:
  - vManage server logs
  - appserver logs
  - service-proxy logs

RECOMMENDATIONS:

- Upgrade Cisco Catalyst SD-WAN Manager to a fixed release immediately.
- Restrict internet exposure of SD-WAN Manager instances wherever possible.
- Review user accounts and remove unnecessary or inactive accounts.
- Monitor logs for signs of suspicious file uploads and unauthorized access.
- Investigate for the presence of "suspicious.war" and related malicious activity.
- Investigate systems for indicators of compromise and engage Cisco TAC if compromise is suspected.

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-arbfw-c2rZvQ