مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Cisco Catalyst SD-WAN Manager

Tracking #:432318982

Date:18-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Cisco Catalyst SD-WAN Manager (formerly SD-WAN vManage) could allow remote attackers to access sensitive information, escalate privileges, or gain unauthorized administrative control over affected systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-20224 | Critical | CVSS 8.6**
  - An XML External Entity (XXE) injection vulnerability in the Cisco Catalyst SD-WAN Manager web UI could allow an unauthenticated remote attacker to read arbitrary files on the affected system by sending crafted XML requests. Successful exploitation may expose sensitive files, credentials, or configuration data.
- **CVE-2026-20209 | Medium | CVSS 5.4**
  - A privilege escalation vulnerability caused by sensitive session information being recorded in audit logs could allow an authenticated attacker with read-only permissions to elevate privileges and perform actions as a high-privileged user.
- **CVE-2026-20210 | Medium | CVSS 5.4**
  - A privilege escalation vulnerability caused by improper redaction of sensitive information in device configurations and templates could allow an authenticated attacker with read-only access to gain elevated privileges and modify system configurations.

Affected Products

Cisco Catalyst SD-WAN Manager across all deployment models, including:

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

Fixed Versions

Cisco Catalyst SD-WAN

- Earlier than 20.9 → Migrate to a fixed release
- 20.9 → 20.9.9.1
- 20.10 → 20.12.7.1
- 20.11 → 20.12.7.1
- 20.12 → 20.12.5.4 / 20.12.6.2 / 20.12.7.1
- 20.13 → 20.15.5.2
- 20.14 → 20.15.5.2
- 20.15 → 20.15.4.4 / 20.15.5.2
- 20.16 → 20.18.2.2
- 20.18 → 20.18.2.2
- 26.1 → 26.1.1.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Cisco.

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-mltvnps2-JxpWm7R