DJ-CERT
Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 19-05-2026

BULLETIN ALERTES

Object	Vulnérabilité dans Cisco Catalyst SD-WAN Controller
Réference	1474
Date de Publication	2026-05-19
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance
- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité

SYSTÉME AFFECTÉ :

Cisco Catalyst SD-WAN Controller et **Cisco Catalyst SD-WAN Manager** (anciennement vSmart et vManage).

Cette vulnérabilité affecte **toutes les versions** suivantes (sauf les versions corrigées) :

- Toutes les versions antérieures à 20.9
- **20.9** ? versions antérieures à **20.9.9.1**
- **20.10** ? versions antérieures à **20.12.7.1**
- **20.11** ? versions antérieures à **20.12.7.1**
- **20.12** ? versions antérieures à **20.12.5.4**, **20.12.6.2** et **20.12.7.1**
- **20.13** ? versions antérieures à **20.15.5.2**
- **20.14** ? versions antérieures à **20.15.5.2**
- **20.15** ? versions antérieures à **20.15.4.4** et **20.15.5.2**
- **20.16** ? versions antérieures à **20.18.2.2**
- **20.18** ? versions antérieures à **20.18.2.2**
- **26.1** ? versions antérieures à **26.1.1.1**

Note : Elle touche **tous les types de déploiement** (On-Premise, Cloud, Government/FedRAMP).

DÉSCRIPTION :

CVE-2026-20182 est une vulnérabilité critique de contournement d'authentification (CWE-287). Elle permet à un attaquant non authentifié de bypasser l'authentification du mécanisme de peering et d'obtenir des privilèges administrateurs.

Cette faille se situe dans le service **vdaemon** lors du handshake du plan de contrôle (port UDP 12346). L'attaquant envoie une séquence de messages DTLS spécialement craftée pendant le handshake de peering. En exploitant une vérification manquante dans le traitement du message CHALLENGE_ACK (lorsque le device type est falsifié), il parvient à faire passer la connexion en état « authentifié » sans vérification valide. Une fois authentifié comme peer légitime, il peut injecter une clé SSH publique dans le compte **vmanage-admin** via NETCONF (TCP 830), modifier la configuration SD-WAN (OMP, TLOC, routes), escalader les privilèges jusqu'à root et installer des backdoors persistants.

NB : cette vulnérabilité est activement exploitée.

SOLUTION :

Appliquer immédiatement les correctifs Cisco publiés le 15/05/2026 pour Cisco Catalyst SD-WAN Controller et SD-WAN Manager, disponibles via le portail Cisco Software Center.

DOCUMENTATION :

• Advisory Cisco officiel — CVE-2026-20182 — https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-auth-rce-cVrhsL5B

• NVD — CVE-2026-20182 — https://nvd.nist.gov/vuln/detail/CVE-2026-20182

• Rapid7 Labs — Analyse technique — https://www.rapid7.com/blog/post/ve-cve-2026-20182-critical-authentication-bypass-cisco-catalyst-sd-wan-controller-fixed/

• CISA KEV — https://www.cisa.gov/known-exploited-vulnerabilities-catalog