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

Autorité Nationale de Cybersécurité

Djibouti le, 10-06-2026

BULLETIN ALERTES

Object	Vulnérabilités critiques dans Cisco Catalyst SD-WAN Manager (vManage)
Réference	1482
Date de Publication	2026-06-10
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire (command injection en root)
- Contournement d'authentification
- Prise de contrôle administrative complète
- Atteinte à la confidentialité, intégrité et disponibilité des données

SYSTÉME AFFECTÉ :

Cisco Catalyst SD-WAN Manager (anciennement vManage).

- 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
- Versions plus récentes jusqu'aux correctifs de mai/juin 2026 (voir advisory Cisco)

DÉSCRIPTION :

CVE-2026-20182 (CVSS 10.0) et **CVE-2026-20127** (CVSS 10.0) : Vulnérabilités de contournement d'authentification (CWE-287) dans le mécanisme de peering (service vdaemon, port UDP 12346). Un attaquant non authentifié peut bypasser l'authentification en envoyant des messages DTLS spécialement conçus pendant le handshake. Cela permet d'obtenir des privilèges administrateurs, d'injecter une clé SSH publique dans le compte vmanage-admin via NETCONF (TCP 830) et de modifier la configuration SD-WAN.

CVE-2026-20245 (CVSS 7.8) : Injection de commandes / élévation de privilèges dans le CLI. Un attaquant authentifié (ou ayant exploité les vulnérabilités précédentes) avec des privilèges netadmin peut exécuter des commandes arbitraires en root via un fichier crafté.

Ces vulnérabilités sont souvent chaînées et **activement exploitées** en 2026.

SOLUTION :

- Appliquer **immédiatement** les correctifs Cisco publiés en mai et juin 2026 via le Cisco Software Center.
- Collecter les request admin-tech sur tous les composants de contrôle **avant** la mise à jour pour préserver les IOC.
- Vérifier les logs et la configuration après mise à jour.
- Suivre les recommandations de remédiation Cisco TAC en cas de compromission confirmée.

DOCUMENTATION :

- Cisco Security Advisory – CVE-2026-20245 (Privilege Escalation) : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrdzx
- Cisco Security Advisory – CVE-2026-20182 (Authentication Bypass) : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
- Cisco Security Advisory – CVE-2026-20127 : https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- Guide de remédiation Catalyst SD-WAN (incluant request admin-tech et TAC) : https://www.cisco.com/c/en/us/support/docs/routers/sd-wan/225842-remediate-catalyst-sd-wan-security.html
- CISA KEV Catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog