AVIS DE SECURITE

Objet	**Multiples vulnérabilités critiques d'exécution de code à distance dans Cisco NX-OS (Nexus 3000/9000) et Cisco UCS**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-256
TLP	WHITE

Résumé

Cisco a publié le 07/10/2026 (mise à jour du 08/10/2026) plusieurs bulletins de sécurité corrigeant des vulnérabilités d'exécution de code à distance sans authentification dans NX-OS : NX-API (CVE-2026-76471), NGOAM (CVE-2026-76485, CVE-2026-76486, CVE-2026-76501) et MPLS OAM (CVE-2026-76465), toutes notées 9.8 (CVSS v3.1, critique). Ces vulnérabilités affectent les commutateurs Nexus 3000 et Nexus 9000 en mode NX-OS autonome ainsi que les UCS 6300 Series Fabric Interconnects, lorsque les fonctionnalités concernées sont activées. Cisco n'a connaissance d'aucune exploitation active ; les failles ont été découvertes lors de tests internes. Le même lot de bulletins corrige 30 CVE dans d'autres produits Cisco (APIC, Meraki, UCS Software, Finesse, Unified CCX/CCE, License On-Prem).

Risque de sécurité

- Exécution de code arbitraire à distance, sans authentification
- Atteinte à la confidentialité des données
- Atteinte à l'intégrité des données
- Déni de service à distance

Systèmes affectés

- Cisco Nexus 3000 Series Switches et Nexus 9000 Series Switches en mode NX-OS autonome (versions NX-OS vulnérables selon le Cisco Software Checker ; fonctionnalités NX-API, NGOAM ou MPLS OAM activées)
- Cisco UCS 6300 Series Fabric Interconnects (UCS Software 4.3 antérieures à 4.3(6j) ; 4.2 et antérieures : migration vers une version corrigée)
- Cisco NX-OS : 10.3 et antérieures avant 10.3(10) ; 10.4 avant 10.4(8) ; 10.5 avant 10.5(6) ; 10.6 avant 10.6(4) ; 9.x avant 9.4(5a) ; 8.x avant 8.4(14)
- Autres produits Cisco concernés par le lot de bulletins : APIC 6.0/6.1/6.2, Meraki (MR, MS, MX, MG, MV, Campus Gateway), UCS Software 6.0 avant 6.0(2e), Finesse, Unified CCX, Packaged/Unified CCE, License On-Prem
- Non affectés : Nexus 7000, Nexus 9000 en mode ACI, MDS 9000, Firepower/Secure Firewall, UCS 6400/6500/6600

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 07/10/2026 :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-napi-rce-r2shwu2j
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngoam-rce-LWKQ4BU
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-moam-rce-uBTzYV7

2. Mettre à jour NX-OS et UCS vers une version corrigée (vérification via le Cisco Software Checker)
3. À défaut de mise à jour immédiate : désactiver les fonctionnalités non nécessaires (« no feature ngoam », « no feature mpls oam », NX-API) ou appliquer les shields Live Protect fournis par Cisco (mesure temporaire)

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar https://www.stcc-ssi.sn/	E-mail : sncsirt@dcssi.sn	Date de publication : 12/10/2026