AVIS DE SECURITE

Objet	**Multiples vulnérabilités critiques dans les produits Cisco (Expressway, Unified Communications, Secure FTD, IOS XE, IOS XR, Snort 3)**
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-278
TLP	WHITE

Résumé

Cisco a publié le 21 octobre 2026 plusieurs avis de sécurité. CVE-2026-76466 (CVSS v3.1 9.8) permet à un attaquant non authentifié d'exécuter des commandes arbitraires en tant que root sur Cisco Expressway (clusters), sans contournement possible. L'avis Unified Communications (cisco-sa-voice-hardening-twgbH9e3) corrige des failles jusqu'à 9.8 (CVE-2026-76473, CVE-2026-76474). Cisco n'a connaissance d'aucune exploitation à ce jour.

Risque de sécurité

- Exécution de code arbitraire à distance (root)
- Contournement de la politique de sécurité (authentification)
- Élévation de privilèges
- Atteinte à la confidentialité et à l'intégrité des données
- Injection SQL et XSS
- Déni de service à distance

Systèmes affectés

- Cisco Expressway Series (Core/Edge) versions antérieures à X15.5.20 (X14 et antérieures : migration requise)
- Cisco Unified CM, Unified CM IM&P, Unified CM SME, Unity Connection, Emergency Responder, Prime Collaboration Deployment : release 14 (migration requise) et release 15 antérieure à 15SU5
- Cisco Secure Firewall Threat Defense (FTD) 7.0.x < 7.0.10, 7.2.x < 7.2.12, 7.4.x < 7.4.8, 7.6.x < 7.6.6, 7.7.x < 7.7.13, 10.0.x < 10.0.2, 10.1.x < 10.1.0
- Cisco IOS XE 17.12.x < 17.12.8, 17.15.x < 17.15.6, 17.18.x < 17.18.5, 26.1.x < 26.1.2, 26.2.x < 26.2.1
- Cisco IOS XR (24.1 à 24.4, 7.9 à 7.11),
- Cyber Vision < 5.6.0,
- Snort 3 < 3.12.4.0,
- Secure Client (versions à vérifier auprès de Cisco)

Recommandations

Se référer aux bulletins de sécurité de l'éditeur du 21/10/2026 :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-hardening-twgbH9e3
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-exwy-hardening-FhcqBVcs
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr9k-tUyxcyXN
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sec-client-priv-esc-muF8eZdm

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar https://www.stcc-ssi.sn/	E-mail : sncsirt@dcssi.sn	Date de publication : 23/10/2026