AVIS DE SECURITE

Objet	**Vulnérabilité exploitée dans Palo Alto Networks PAN-OS (CVE-2026-0322) et multiples vulnérabilités dans les produits Palo Alto Networks**
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2026-ADS-263
TLP	WHITE

Résumé

Palo Alto Networks a publié le 14/10/2026 des correctifs pour plusieurs vulnérabilités (CVE-2026-0311 à CVE-2026-0322) affectant PAN-OS, Panorama, Prisma Access, GlobalProtect, Checkov, Cortex XSOAR/XSIAM et Prisma Browser. La vulnérabilité CVE-2026-0322 (CVSS v3.1 : 7.2), permettant à un administrateur authentifié d'exécuter du code arbitraire en tant que root via l'interface de gestion de PAN-OS, est activement exploitée selon l'éditeur. L'éditeur a également publié le bulletin PAN-SA-2026-0013 relatif aux correctifs Chromium de Prisma Browser.

Risque de sécurité

- Exécution de code arbitraire à distance
- Contournement de la politique de sécurité
- Déni de service à distance
- Élévation de privilèges
- Injection de code indirecte à distance (XSS)
- Falsification de requêtes côté serveur (SSRF)

Systèmes affectés

- PAN-OS (PA-Series, VM-Series, Panorama) : toutes versions antérieures à 11.2.16 et à 12.2.4, ainsi que les branches 10.2, 11.1, 12.1 antérieures aux correctifs cumulatifs (ex. 10.2.18-h12, 11.1.16-h3, 12.1.10-h2)
- Prisma Access : versions antérieures à 10.2.0, 11.2.0 et 12.1.0 sans les derniers correctifs de sécurité
- GlobalProtect App : 6.0.x antérieures à 6.0.15, 6.2.x antérieures à 6.2.8-h15, 6.3.x antérieures à 6.3.3-h16
- Checkov by Prisma Cloud : 3.2.x antérieures à 3.2.533, 3.3.x antérieures à 3.3.25
- Cortex XSOAR OS Query et Cortex XSIAM OS Query : versions antérieures à 1.0.17
- Prisma Browser : versions antérieures à 152.8.5.83

Recommandations

1. Se référer aux bulletins de sécurité de l'éditeur du 14/10/2026 :

- https://security.paloaltonetworks.com/CVE-2026-0322
- https://security.paloaltonetworks.com/PAN-SA-2026-0013
- https://security.paloaltonetworks.com/CVE-2026-0311
- https://security.paloaltonetworks.com/CVE-2026-0321

2. Mettre à jour PAN-OS vers une version corrigée sans délai (exploitation active de CVE-2026-0322)
3. Restreindre l'accès à l'interface de gestion de PAN-OS aux seules adresses IP internes de confiance

Adresse : Avenue Leopold S. Senghor, BP: 4026, Dakar https://www.stcc-ssi.sn/	E-mail : sncsirt@dcssi.sn	Date de publication : 16/10/2026