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

Autorité Nationale de Cybersécurité

Djibouti le, 12-07-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans PAN-OS et Prisma Access de Palo Alto Networks
Réference	1491
Date de Publication	2026-07-08
Sévérité	Critique

IMPACT :

- Exécution de commandes arbitraires
- Élévation de privilèges
- Déni de service à distance
- Contournement de mécanismes de sécurité
- Divulgation d'informations
- Atteinte potentielle à la confidentialité et à l'intégrité des données

SYSTÉME AFFECTÉ :

- PAN-OS 12.1 versions antérieures à 12.1.4-h8, 12.1.7-h2, 12.1.8
- PAN-OS 11.2 versions antérieures à 11.2.4-h20, 11.2.7-h18, 11.2.10-h12, 11.2.13
- PAN-OS 11.1 versions antérieures à 11.1.4-h35, 11.1.6-h35, 11.1.7-h8, 11.1.10-h30, 11.1.13-h9, 11.1.16
- PAN-OS 10.2 versions antérieures à 10.2.7-h36, 10.2.10-h39, 10.2.13-h23, 10.2.16-h9, 10.2.18-h8
- Prisma Access 11.2.0 versions antérieures à 11.2.7-h18
- Prisma Access 10.2.0 versions antérieures à 10.2.10-h39

DÉSCRIPTION :

Plusieurs vulnérabilités ont été corrigées dans PAN-OS et Prisma Access de Palo Alto Networks. Selon la vulnérabilité exploitée, un attaquant pourrait exécuter des commandes arbitraires, provoquer un déni de service, contourner certaines fonctions de sécurité, obtenir des privilèges supplémentaires ou accéder à des informations sensibles. Certaines vulnérabilités affectent également les composants Prisma Access, pouvant réduire l'efficacité de certains mécanismes de protection réseau ou de prévention contre la perte de données (DLP).

SOLUTION :

Mettre à jour **PAN-OS** et **Prisma Access** vers les versions corrigées suivantes :

- **PAN-OS 12.1** : 12.1.4-h8, 12.1.7-h2 ou 12.1.8 (ou une version ultérieure)
- **PAN-OS 11.2** : 11.2.4-h20, 11.2.7-h18, 11.2.10-h12 ou 11.2.13 (ou une version ultérieure)
- **PAN-OS 11.1** : 11.1.4-h35, 11.1.6-h35, 11.1.7-h8, 11.1.10-h30, 11.1.13-h9 ou 11.1.16 (ou une version ultérieure)
- **PAN-OS 10.2** : 10.2.7-h36, 10.2.10-h39, 10.2.13-h23, 10.2.16-h9 ou 10.2.18-h8 (ou une version ultérieure)
- **Prisma Access 11.2.0** : 11.2.7-h18 ou une version ultérieure
- **Prisma Access 10.2.0** : 10.2.10-h39 ou une version ultérieure

DOCUMENTATION :

CVE-2026-0277 :

- https://security.paloaltonetworks.com/CVE-2026-0277

CVE-2026-0278 :

- https://security.paloaltonetworks.com/CVE-2026-0278

CVE-2026-0283 :

- https://security.paloaltonetworks.com/CVE-2026-0283

CVE-2026-0284 :

- https://security.paloaltonetworks.com/CVE-2026-0284

CVE-2026-0285 :

- https://security.paloaltonetworks.com/CVE-2026-0285

CVE-2026-0286 :

- https://security.paloaltonetworks.com/CVE-2026-0286

CVE-2026-0287 :

- https://security.paloaltonetworks.com/CVE-2026-0287

CVE-2026-0288 :

- https://security.paloaltonetworks.com/CVE-2026-0288