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

Autorité Nationale de Cybersécurité

Djibouti le, 12-11-2026

BULLETIN ALERTES

Object	Vulnérabilité dans PAN-OS sur Panorama de Palo Alto Networks
Réference	1514
Date de Publication	2026-11-12
Sévérité	Elevé

IMPACT :

- Exécution de code à distance
- Élévation de privilèges
- Atteinte potentielle à la confidentialité, à l'intégrité et à la disponibilité des données

SYSTÉME AFFECTÉ :

- PAN-OS 12.2 sur Panorama versions antérieures à 12.2.4-h2
- PAN-OS 12.1 sur Panorama versions antérieures à 12.1.4-h14, 12.1.7-h12, 12.1.10-h4
- PAN-OS 11.2 sur Panorama versions antérieures à 11.2.4-h24, 11.2.7-h24, 11.2.10-h18, 11.2.13-h5, 11.2.16-h2
- PAN-OS 11.1 sur Panorama versions antérieures à 11.1.4-h39, 11.1.6-h41, 11.1.7-h13, 11.1.10-h37, 11.1.13-h17, 11.1.16-h5
- PAN-OS 10.2 sur Panorama versions antérieures à 10.2.7-h40, 10.2.10-h43, 10.2.13-h28, 10.2.16-h13, 10.2.18-h14

DÉSCRIPTION :

Une vulnérabilité d'injection de code a été corrigée dans le logiciel PAN-OS de Palo Alto Networks lorsqu'il est utilisé sur Panorama. Un administrateur authentifié qui a un accès réseau à l'équipement peut l'exploiter pour exécuter du code arbitraire avec les privilèges root. Aucune configuration particulière n'est nécessaire pour être exposé. Le risque est le plus élevé lorsque l'interface de gestion est accessible depuis Internet. Les pare-feu PAN-OS autonomes, Cloud NGFW et Prisma Access ne sont pas concernés. L'éditeur indique ne pas avoir connaissance d'une exploitation malveillante de cette vulnérabilité.

SOLUTION :

Mettre à jour PAN-OS sur Panorama vers les versions corrigées suivantes :

- PAN-OS 12.2 : 12.2.4-h2 (ou une version ultérieure)
- PAN-OS 12.1 : 12.1.4-h14, 12.1.7-h12 ou 12.1.10-h4 (ou une version ultérieure)
- PAN-OS 11.2 : 11.2.4-h24, 11.2.7-h24, 11.2.10-h18, 11.2.13-h5 ou 11.2.16-h2 (ou une version ultérieure)
- PAN-OS 11.1 : 11.1.4-h39, 11.1.6-h41, 11.1.7-h13, 11.1.10-h37, 11.1.13-h17 ou 11.1.16-h5 (ou une version ultérieure)
- PAN-OS 10.2 : 10.2.7-h40, 10.2.10-h43, 10.2.13-h28, 10.2.16-h13 ou 10.2.18-h14 (ou une version ultérieure)

Versions de PAN-OS qui ne sont plus prises en charge : migrer vers une version prise en charge et corrigée.

DOCUMENTATION :

Bulletin de sécurité Palo Alto Networks

- https://security.paloaltonetworks.com/CVE-2026-0330

CVE-2026-0330 :

- https://www.cve.org/CVERecord?id=CVE-2026-0330