



#### NOTE DE SECURITE

|                            |   |
|----------------------------|---|
| <b>Titre</b>               | Une vulnérabilité potentielle d'exécution de code à distance via l'interface de gestion de PAN-OS |
| <b>Numéro de Référence</b> | 50701211/24   |
| <b>Date de Publication</b> | 12 Novembre 2024  |
| <b>Risque</b>              | Important   |
| <b>Impact</b>              | Important   |

Palo Alto Networks a publié un bulletin d'information important concernant une vulnérabilité potentielle liée à l'interface de gestion des appareils PAN-OS. Une revendication d'une vulnérabilité d'exécution de code à distance a été identifiée de manière externe, mais les détails du problème sont actuellement inconnus. À titre de précaution, Palo Alto Networks recommande fortement à ses clients de s'assurer que leurs interfaces de gestion sont sécurisées conformément aux meilleures pratiques. La vulnérabilité pourrait exposer les appareils dont les interfaces de gestion ne sont pas correctement restreintes aux adresses IP internes de confiance, augmentant ainsi le risque d'accès non autorisé et d'exploitation potentielle. Bien qu'aucune exploitation n'ait été observée à ce jour, Palo Alto Networks recommande de suivre ses bonnes pratiques et ses recommandations de sécurité pour la gestion et la sécurisation de l'interface de gestion des appareils PAN-OS.

#### Références :

Bulletin de sécurité Palo Alto 11 Novembre 2024:

- <https://security.paloaltonetworks.com/PAN-SA-2024-0015>

How to Secure the Management Access of Your Palo Alto Networks Device:

- <https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431>