



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité critique dans Palo Alto PAN-OS
<b>Numéro de Référence</b>	51682712/24
<b>Date de Publication</b>	27 Décembre 2024
<b>Risque</b>	Critique
<b>Impact</b>	Critique

### Systemes affectés

- Palo Alto Expedition version antérieure à 1.2.96
- PAN-OS 10.1.x version antérieure à 10.1.14-h8
- PAN-OS 10.1.x version antérieure à 10.2.10-h12
- PAN-OS 10.1.x version antérieure à 11.1.5
- PAN-OS 10.1.x version antérieure à 11.2.3

### Identificateurs externes

- CVE-2024-3393

### Bilan de la vulnérabilité

Palo Alto Networks a corrigée une faille de sécurité critique dans PAN-OS qui affecte la fonction « DNS Security ». L'exploitation de cette faille peut permettre à un attaquant non authentifiés de perturber le fonctionnement des pare-feu et de les forcer à passer en mode de maintenance via l'envoi d'un paquet malveillant spécialement conçu, ce qui provoque un redémarrage du pare-feu et peut entraîner un déni de service.

### Solution

Veillez se référer au bulletin de sécurité Palo Alto du 27 Décembre 2024.

### Risque

- Déni de service

### Annexe

Bulletin de sécurité Palo Alto du 27 Décembre 2024:

- <https://security.paloaltonetworks.com/CVE-2024-3393>