



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités dans Palo Alto PAN-OS
<b>Numéro de Référence</b>	46111602/24
<b>Date de Publication</b>	16 Février 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- PAN-OS 11.0.x version antérieure à 11.0.3
- PAN-OS 10.2.x version antérieure à 10.2.6
- PAN-OS 10.1.x version antérieure à 10.1.11
- PAN-OS 9.1.x version antérieure à 9.1.16

### Identificateurs externes

- CVE-2024-00010 CVE-2024-0007 CVE-2024-0008 CVE-2024-0009 CVE-2024-0010  
CVE-2024-0011

### Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les versions susmentionnées de Palo Alto PAN-OS. L'exploitation de ces failles peut permettre à un attaquant de provoquer une injection de code indirecte à distance (XSS) et un contournement de la politique de sécurité.

### Solution

Veillez se référer au bulletin de sécurité Palo Alto du 14 Février 2024.

### Risque

- Injection de code indirecte à distance (XSS)
- Contournement de la politique de sécurité

### Annexe

Bulletin de sécurité Palo Alto du 14 Février 2024:

- <https://security.paloaltonetworks.com/CVE-2024-00010>
- <https://security.paloaltonetworks.com/CVE-2024-0007>
- <https://security.paloaltonetworks.com/CVE-2024-0008>
- <https://security.paloaltonetworks.com/CVE-2024-0009>
- <https://security.paloaltonetworks.com/CVE-2024-0011>