



BULLETIN DE SECURITE

Titre	Vulnérabilités dans Palo Alto PAN-OS et Networks GlobalProtect app
Numéro de Référence	42431506/23
Date de Publication	15 Juin 2023
Risque	Important
Impact	Important

Systemes affectés

- PAN-OS 10.2.x
- PAN-OS 10.1.x
- PAN-OS 10.x
- PAN-OS 9.1.x
- PAN-OS 9.0.x
- PAN-OS 8.1.x
- Palo Alto Networks GlobalProtect app 6.1.x versions antérieures à 6.1.1
- Palo Alto Networks GlobalProtect app 6.0.x versions antérieures à 6.0.5
- Palo Alto Networks GlobalProtect app 5.2.x versions antérieures à 5.2.13

Identificateurs externes

- CVE-2023-0009, CVE-2023-0010

Bilan de la vulnérabilité

Deux vulnérabilités ont été corrigées dans les versions susmentionnées de Palo Alto PAN-OS et Networks GlobalProtect app. L'exploitation de ces failles peut permettre à un attaquant de porter atteinte à la confidentialité des données, de réussir une injection de code indirecte à distance (XSS) et une élévation de privilèges.

Solution

Veillez se référer au bulletin de sécurité Palo Alto du 14 Juin 2023.

Risque

- Atteinte à la confidentialité des données
- Injection de code indirecte à distance
- Elévation de privilèges

Annexe

Bulletin de sécurité Palo Alto du 14 Juin 2023:

- <https://security.paloaltonetworks.com/CVE-2023-0009>
- <https://security.paloaltonetworks.com/CVE-2023-0010>