

Agence Nationale
des Systèmes d'information
de l'état

Djibouti le, 15-04-2025

BULLETIN ALERTES

Object	Vulnérabilités critiques dans les produits Palo Alto
Référence	1341
Date de Publication	2025-04-14
Sévérité	Critique

IMPACT :

- Atteinte à l'intégrité des données
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire
- Non spécifié par l'éditeur
- Élévation de privilèges

SYSTÈME AFFECTÉ :

- Cloud NGFW sans les derniers correctifs de sécurité
- Cortex XDR Agent versions 7.9-CE.x antérieures à 7.9.103-CE HF pour Windows
- Cortex XDR Agent versions 8.3-CE.x antérieures à 8.3.101-CE HF pour Windows
- Cortex XDR Agent versions 8.5.x antérieures à 8.5.2 pour Windows
- Cortex XDR Agent versions 8.6.x antérieures à 8.6.1 pour Windows
- Cortex XDR Broker VM versions antérieures à 26.100.3
- GlobalProtect App versions 6.3.x antérieures à 6.3.3 pour Windows
- GlobalProtect App versions 6.x antérieures à 6.2.8 pour Windows
- PAN-OS versions 10.1.x antérieures à 10.1.14-h13
- PAN-OS versions 10.2.x antérieures à 10.2.15
- PAN-OS versions 11.0.x antérieures à 11.0.6
- PAN-OS versions 11.1.x antérieures à 11.1.8
- PAN-OS versions 11.2.x antérieures à 11.2.6
- Prisma Access Browser versions antérieures à 132.83.3017.1
- Prisma Access versions 10.2.10.x antérieures à 10.2.10-h16
- Prisma Access versions 10.2.4.x antérieures à 10.2.4-h36
- Prisma Access versions 11.2.x antérieures à 11.2.4-h5
- Prisma SD-WAN versions 6.1.x antérieures à 6.1.10
- Prisma SD-WAN versions 6.2.x et 6.3.x antérieures à 6.3.4
- Prisma SD-WAN versions 6.4.x antérieures à 6.4.2
- Prisma SD-WAN versions 6.5.x antérieures à 6.5.1

DÉSCRIPTION :

Plusieurs vulnérabilités ont été identifiées dans les produits Palo Alto Networks. Certaines d'entre elles pourraient être exploitées par un attaquant afin d'exécuter du code arbitraire, d'obtenir une élévation de privilèges ou de provoquer un déni de service à distance.

SOLUTION :

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).



DOCUMENTATION :

- Bulletin de sécurité Palo Alto Networks CVE-2025-0119 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0119>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0120 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0120>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0121 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0121>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0122 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0122>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0123 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0123>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0124 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0124>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0125 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0125>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0126 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0126>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0127 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0127>

- Bulletin de sécurité Palo Alto Networks CVE-2025-0128 du 09 avril 2025

<https://security.paloaltonetworks.com/CVE-2025-0128>

- Bulletin de sécurité Palo Alto Networks PAN-SA-2025-0008 du 09 avril 2025

<https://security.paloaltonetworks.com/PAN-SA-2025-0008>

- CVE-2025-0119

<https://www.cve.org/CVERecord?id=CVE-2025-0119>



- CVE-2025-0120

<https://www.cve.org/CVERecord?id=CVE-2025-0120>

- CVE-2025-0121

<https://www.cve.org/CVERecord?id=CVE-2025-0121>

- CVE-2025-0122

<https://www.cve.org/CVERecord?id=CVE-2025-0122>

- CVE-2025-0123

<https://www.cve.org/CVERecord?id=CVE-2025-0123>

- CVE-2025-0124

<https://www.cve.org/CVERecord?id=CVE-2025-0124>

- CVE-2025-0125

<https://www.cve.org/CVERecord?id=CVE-2025-0125>

- CVE-2025-0126

<https://www.cve.org/CVERecord?id=CVE-2025-0126>

- CVE-2025-0127

<https://www.cve.org/CVERecord?id=CVE-2025-0127>

- CVE-2025-0128

<https://www.cve.org/CVERecord?id=CVE-2025-0128>

- CVE-2025-0129

<https://www.cve.org/CVERecord?id=CVE-2025-0129>

- CVE-2025-1920

<https://www.cve.org/CVERecord?id=CVE-2025-1920>

- CVE-2025-2135

<https://www.cve.org/CVERecord?id=CVE-2025-2135>

- CVE-2025-2136

<https://www.cve.org/CVERecord?id=CVE-2025-2136>

- CVE-2025-2137

<https://www.cve.org/CVERecord?id=CVE-2025-2137>

- CVE-2025-2476

<https://www.cve.org/CVERecord?id=CVE-2025-2476>

- CVE-2025-2783

<https://www.cve.org/CVERecord?id=CVE-2025-2783>