ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans Palo Alto Networks
Numéro de Référence	47881206/24
Date de Publication	13 Juin 2024
Risque	Important
Impact	Important

Systèmes affectés

- Prisma Cloud Compute versions 32.x antérieures à 32.05 (O'Neal - Update 5)
- GlobalProtect App versions 6.2.x antérieures à 6.2.3
- GlobalProtect App versions 6.1.x antérieures à 6.1.3
- GlobalProtect App versions 6.0.x antérieures à 6.0.8
- GlobalProtect App versions 5.1.x antérieures à 5.1.12
- Cortex XDR Agent versions 8.3.x antérieures à 8.3.1 sur Windows
- Cortex XDR Agent versions 8.1.x à 8.2.x antérieures à 8.2.1 sur Windows
- Cortex XDR Agent versions 7.9.x.-CE antérieures à 7.9.102-CE sur Windows

Identificateurs externes

- CVE-2024-5905 CVE-2024-5906 CVE-2024-5907 CVE-2024-5908 CVE-2024-5909

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits susmentionnés de Palo Alto Networks. L'exploitation de ces failles peut permettre à un attaquant de réussir une élévation de privilèges, d'injecter du code indirect à distance (XSS) et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Palo Alto du 12 Juin 2024**.**

Risque

- Atteinte à la confidentialité des données
- Injection de code indirect à distance (XSS)

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- Elévation de privilèges

Annexe

Bulletin de sécurité Palo Alto du 12 Juin 2024**:**

- https://security.paloaltonetworks.com/CVE-2024-5905
- https://security.paloaltonetworks.com/CVE-2024-5906
- https://security.paloaltonetworks.com/CVE-2024-5907
- https://security.paloaltonetworks.com/CVE-2024-5908
- https://security.paloaltonetworks.com/CVE-2024-5909