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	Vulnérabilité critique dans FortiOS
Numéro de Référence	45940902/24
Date de Publication	09 Février 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiOS 7.4 de 7.4.0 à 7.4.2
- FortiOS 7.2 de 7.2.0 à 7.2.6
- FortiOS 7.0 de 7.0.0 à 7.0.13
- FortiOS 6.4 de 6.4.0 à 6.4.14
- FortiOS 6.2 de 6.2.0 à 6.2.15
- FortiOS 6.0 toutes les versions

Identificateurs externes

- CVE-2024-21762

Bilan de la vulnérabilité

Fortinet avertit qu'une nouvelle vulnérabilité critique d'exécution de code à distance dans FortiOS SSL VPN est potentiellement exploitée dans des attaques. L'exploitation de la faille (CVE-2024-21762 / FG-IR-24-015) permet à des attaquants non authentifiés d'obtenir une exécution de code à distance (RCE) via des requêtes malicieusement conçues.

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 08 Février 2024 pour plus d'information.

Risque

- Exécution de code à distance

Annexe

Bulletin de sécurité Fortinet du 08 Février 2024:

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

- https://www.fortiguard.com/psirt/FG-IR-24-015