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	Post-exploitation attaque via des liens symboliques cible des dispositifs FortiGate
Numéro de Référence	53981404/25
Date de Publication	14 Avril 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiOS versions 7.6.x antérieures à 7.6.2
- FortiOS versions 7.4.x antérieures à 7.4.7
- FortiOS versions 7.2.x antérieures à 7.2.11
- FortiOS versions 7.0.x antérieures à 7.0.17
- FortiOS versions 6.x antérieures à 6.4.16

Identificateurs externes

- CVE-2022-42475 CVE-2023-27997 CVE-2024-21762

Bilan de la vulnérabilité

Fortinet a identifié une technique d'exploitation « post-exploitation » utilisée par un acteur malveillant ciblant des dispositifs FortiGate vulnérables via des failles connues non corrigées. L'attaquant a exploité des vulnérabilités connues (FG-IR-22-398, FG-IR-23-097, FG-IR-24-015) préexistante pour conserver un accès en lecture seule en créant un lien symbolique entre le système de fichiers utilisateur et celui du système, spécifiquement dans le répertoire servant les fichiers de langue du SSL-VPN.

En résumé, même après la mise à jour des dispositifs vers des versions corrigées de FortiOS, un lien symbolique laissé par l'attaquant peut lui permettre d'éviter la détection et de maintenir un accès en lecture seule aux fichiers du système, notamment aux configurations sensibles.

Ce vecteur d'attaque permet un accès non autorisé et persistant aux fichiers de configuration du système, avec des risques potentiels de fuite de données sensibles. Il existe également une possibilité de compromission supplémentaire si cet accès est combiné à d'autres vulnérabilités. Toutefois, seuls les dispositifs ayant activé le SSL-VPN et ayant été précédemment vulnérables aux CVE susmentionnés sont concernés.

Fortinet a déployé plusieurs mesures correctives pour remédier à cette technique d'exploitation :

- Une signature AV/IPS a été créée pour détecter et supprimer ce lien symbolique des appareils concernés ;
- Des modifications ont été apportées aux dernières versions afin de détecter et de supprimer le lien symbolique et de s'assurer que le VPN SSL ne sert que les fichiers autorisés;

Solution

Veuillez se référer au bulletin de sécurité Fortinet du 10 Avril 2025 afin d'installer les nouvelles mises à jour.

Risque

- Atteinte à la confidentialité de données,
- Fuite de données,

Annexe

Bulletins de sécurité Fortinet du 10 Avril 2025 :

- https://www.fortinet.com/blog/psirt-blogs/analysis-of-threat-actor-activity

Bulletins de sécurité Fortinet du 22 Dec 2022 :

- https://www.fortiguard.com/psirt/FG-IR-22-398

Bulletins de sécurité Fortinet du 12 Juin 2023 :

- https://www.fortiguard.com/psirt/FG-IR-23-097

Bulletins de sécurité Fortinet du 15 Janvier 2025 :

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

Bulletins de sécurité DGSSI:

- https://www.dgssi.gov.ma/fr/bulletins/mise-jour-de-securite-pour-fortinet-fortios
- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilite-critique-affectant-fortinet-fortios
- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilite-critique-dans-fortios