



NOTE D'INFORMATION

Titre	Publication d'exploit de la vulnérabilité « CVE-2022-40684 » affectant les produits Fortinet
Numéro de Référence	38691410/22
Date de Publication	14 Octobre 2022
Risque	Critique
Impact	Critique

Un code d'exploit est publiquement disponible de la vulnérabilité critique "CVE-2022-40684" de contournement d'authentification affectant les appliances FortiOS, FortiProxy et FortiSwitchManager de Fortinet.

Les attaquants peuvent utiliser cette vulnérabilité pour compromettre davantage les systèmes vulnérables en :

- Modifiant les clés SSH des utilisateurs admin pour permettre à l'attaquant de se connecter au système compromis.
- Ajoutant de nouveaux utilisateurs locaux.
- Mettant à jour les configurations de réseau pour réacheminer le trafic.
- Téléchargeant la configuration du système.
- Initiant des captures de paquets pour capturer d'autres informations sensibles du système.

Il est fortement recommandé d'appliquer immédiatement les correctifs de sécurité ou désactiver les appareils vulnérables pour s'assurer que les serveurs ne sont pas compromis. En outre, si l'application de la mise à jour de sécurité ou la désactivation des appareils s'avère impossible, il est recommandé d'utiliser les mesures d'atténuation partagées par Fortinet dans [cet avis de sécurité](#).

Annexe

Bulletins de sécurité maCERT du 11 Octobre 2022:

- <https://dgssi.gov.ma/fr/content/3858071022-vulnerabilite-critique-dans-les-produits-fortinet.html>

Bulletins de sécurité Fortinet du 10 Octobre 2022:

- <https://www.fortiguard.com/psirt/FG-IR-22-377>