CERT.tg : ANNONCE DE SÉCURITÉ **Date** : 09/03/2023

Type de Contenu	Description
Titre	*Vulnérabilité critique sur les produits FortiOS et Fortiproxy de Fortinet*
ID	*202303/AS/05*
Code TLP	*Green*
Niveau de Risque	*Critique*
Application et service affectés	***FortiOS et FortiProxy***
Version / Edition	- *FortiOS version 7.2.0 à 7.2.3,* - *FortiOS version 7.0.0 à 7.0.9,* - *FortiOS version 6.4.0 à 6.4.11* - *FortiOS version 6.2.0 à 6.2.12* - *FortiOS version 6.0 toutes les versions* - *FortiProxy version 7.2.0 à 7.2.2,* - *FortiProxy version 7.0.0 à 7.0.8* - *FortiProxy version 2.0.0 à 2.0.11,* - *FortiProxy 1.2 toutes les versions* - *FortiProxy and 1.1 toutes les versions*
Plateforme	***Fortinet***
Mise à jour	- *FortiOS version 7.4.0 ou supérieure* - *FortiOS version 7.2.4 ou supérieure* - *FortiOS version 7.0.10 ou supérieure* - *FortiOS version 6.4.12 ou supérieure* - *FortiOS version 6.2.13 ou supérieure* - *FortiProxy version 7.2.3 ou supérieure* - *FortiProxy version 7.0.9 ou supérieure* - *FortiProxy version 2.0.12 ou supérieure* - *FortiOS-6K7K version 7.0.10 ou supérieure* - *FortiOS-6K7K version 6.4.12 ou supérieure* - *FortiOS-6K7K version 6.2.13 ou supérieure*
Résumé	*La vulnérabilité permet à un attaquant non authentifié d'exécuter un code arbitraire ou d'effectuer un déni de service sur l'interface graphique des appareils vulnérables en utilisant des requêtes spécialement conçues.*
Impacts	- ***Exécution de code arbitraire ou de déni de service*** - ***Fuites de données sensibles*** - ***Corruption de données***

Description Détaillée	*La faille identifiée comme **CVE-2023-25610** est une vulnérabilité de type "buffer underflow" qui se produit lorsqu'un programme tente de lire plus de données à partir d'une mémoire tampon que ce qui est disponible, ce qui entraîne l'accès à des emplacements de mémoire adjacents, conduisant à un comportement risqué ou à des plantages.*
Solutions	*Pour résoudre le problème, il faut faire une mise à jour de vos appareils concernés vers les versions dans lesquelles la vulnérabilité est corrigée.* *Si vous êtes dans l'incapacité d'appliquer ces mises à jour, vous pouvez désactiver l'interface administrative HTTP/HTTPS ou limiter les adresses IP qui peuvent atteindre ces équipements.*
Liens pour plus de détails	*https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-25610* *https://thehackernews.com/2023/03/new-critical-flaw-in-fortios-and.html* *https://www.fortiguard.com/psirt/FG-IR-23-001*