



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité dans Fortinet FortiOS
<b>Numéro de Référence</b>	26001707/20
<b>Date de Publication</b>	17 juillet 2020
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- FortiOS 6.4.x versions antérieures à 6.4.1 ;
- FortiOS 6.2.x versions antérieures à 6.2.4 ;
- FortiOS 6.0.x versions antérieures à 6.0.10 ;

### Identificateurs externes

- CVE-2020-12812;

### Bilan de la vulnérabilité

Fortinet a corrigé une vulnérabilité dans FortiOS. La vulnérabilité est due à une erreur dans le traitement des demandes d'authentification dans SSL VPN. Un attaquant authentifié à distance peut modifier la casse de son nom d'utilisateur afin d'obtenir un accès non autorisé à l'application sans être invité à entrer le deuxième facteur d'authentification (FortiToken).

### Solution

Veillez-vous référer au bulletin de sécurité Fortinet du 13 Juillet 2020 afin d'installer les nouvelles mises à jour.

### Risque

- Contournement de la politique de sécurité ;

### Référence

Bulletin de sécurité Fortinet du 13 juillet 2020 :

- <https://fortiguard.com/psirt/FG-IR-19-283>