

**ROYAUME DU MAROC**  
**ADMINISTRATION**  
**DE LA DEFENSE NATIONALE**  
**Direction Générale de la Sécurité**  
**des Systèmes d'Information**  
.....  
**Centre de Veille de Détection et de**  
**Réaction aux Attaques Informatiques**



المملكة المغربية  
ادارة الدفاع الوطني  
المديرية العامة لأمن نظم المعلومات  
مركز اليقظة والرصد والتصدي  
للهجمات المعلوماتية

**BULLETIN DE SECURITE**

<b>Titre</b>	Vulnérabilités affectant des produits de Fortinet
<b>Numéro de Référence</b>	60981102/26
<b>Date de publication</b>	11 février 2026
<b>Risque</b>	Important
<b>Impact</b>	Important

**Systèmes affectés**

- FortiOS 6.4 toutes les versions
- FortiOS 7.0 toutes les versions
- FortiOS 7.2 toutes les versions
- FortiOS 7.4.0 jusqu'à la version 7.4.9
- FortiOS 7.6.0 jusqu'à la version 7.6.4
- FortiSandbox 5.0 de 5.0.0 jusqu'à 5.0.1
- FortiSandbox 4.4 de 4.4.0 jusqu'à 4.4.7
- FortiSandbox 4.2 toutes les versions
- FortiSandbox 4.0 toutes les versions
- FortiAuthenticator de 6.6.0 jusqu'à 6.6.6
- FortiAuthenticator 6.5 toutes les versions
- FortiAuthenticator 6.4 toutes les versions
- FortiAuthenticator 6.3 toutes les versions
- FortiClientWindows 7.4 de 7.4.0 jusqu'à 7.4.4
- FortiClientWindows 7.2 de 7.2.0 jusqu'à 7.2.12
- FortiClientWindows 7.0 toutes les versions

## **Identificateurs externes**

- CVE-2025-62439 CVE-2025-64157 CVE-2026-22153 CVE-2025-55018
- CVE-2025-68686 CVE-2025-52436 CVE-2025-62676 CVE-2026-21743

## **Bilan de la vulnérabilité**

Fortinet annonce la disponibilité de mises à jour de sécurité permettant la correction de plusieurs vulnérabilités affectant les versions susmentionnées de ses produits « FortiSandbox » et « FortiOS ». L'exploitation de ces vulnérabilités peut permettre à un attaquant d'exécuter du code à distance, de contourner des mesures de sécurité, d'accéder à des informations confidentielles ou d'injecter du contenu dans une page.

## **Solution**

Veuillez se référer aux bulletins de sécurité de Fortinet pour mettre à jour vos produits.

## **Risques**

- Contournement de mesures de sécurité
- Exécution de code à distance
- Accès à des informations confidentielles
- Injection de contenu dans une page

## **Références**

Bulletins de sécurité de Fortinet:

- <https://www.fortiguard.com/psirt/FG-IR-25-384>
- <https://www.fortiguard.com/psirt/FG-IR-25-795>
- <https://www.fortiguard.com/psirt/FG-IR-25-1052>
- <https://www.fortiguard.com/psirt/FG-IR-25-667>
- <https://www.fortiguard.com/psirt/FG-IR-25-934>
- <https://www.fortiguard.com/psirt/FG-IR-25-093>