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

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Fortinet
Numéro de Référence	59961501/26
Date de publication	15 janvier 2026
Risque	Important
Impact	Critique

Systèmes affectés

- FortiClientEMS 7.0 toutes les versions
- FortiClientEMS 7.2.0 jusqu'à la version 7.2.10
- FortiClientEMS 7.4.0 jusqu'à la version 7.4.1
- FortiClientEMS 7.4.3 jusqu'à la version 7.4.4
- FortiOS 6.4.0 jusqu'à la version 6.4.16
- FortiOS 7.0.0 jusqu'à la version 7.0.17
- FortiOS 7.2.0 jusqu'à la version 7.2.11
- FortiOS 7.4.0 jusqu'à la version 7.4.8
- FortiOS 7.6.0 jusqu'à la version 7.6.3
- FortiSwitchManager 7.0.0 jusqu'à la version 7.0.5
- FortiSwitchManager 7.2.0 jusqu'à la version 7.2.6
- FortiSASE 25.1.a
- FortiSASE 25.2.b
- FortiSIEM 7.4.0
- FortiSIEM de 7.3.0 jusqu'à la version 7.3.4
- FortiSIEM de 7.2.0 jusqu'à la version 7.2.6
- FortiSIEM de 7.1.0 jusqu'à la version 7.1.8
- FortiSIEM de 7.0.0 jusqu'à la version 7.0.4
- FortiSIEM de 6.7.0 jusqu'à la version 6.7.10
- FortiFone de 7.0.0 jusqu'à 7.0.1
- FortiFone de 3.0.13 jusqu'à 3.0.23
- FortiSandbox de la version 5.0.0 jusqu'à 5.0.4
- FortiSandbox 4.4 toutes les versions

- FortiSandbox 4.2 toutes les versions
- FortiSandbox 4.0 toutes les versions

Identificateurs externes

CVE-2025-25249 CVE-2025-59922 CVE-2025-64155 CVE-2025-47855 CVE-2025-67685

Bilan de la vulnérabilité

Fortinet annonce la disponibilité de mises à jour de sécurité permettant la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. Deux de ces vulnérabilités identifiées par « CVE-2025-64155 » et « CVE-2025-47855 » sont critiques. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de contourner des mesures de sécurité, d'injecter du code SQL ou de falsifier des requêtes coté serveur.

Solution

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

Risques

- Contournement de la politique de sécurité
- Exécution de code arbitraire à distance
- Injection de code SQL
- Falsification de requêtes côté serveur

Références

Bulletins de sécurité de Fortinet:

- https://www.fortiguard.com/psirt/FG-IR-25-735
- https://www.fortiguard.com/psirt/FG-IR-25-084
- https://www.fortiguard.com/psirt/FG-IR-25-783

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

- https://www.fortiguard.com/psirt/FG-IR-25-260
- https://www.fortiguard.com/psirt/FG-IR-25-772