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 critiques affectant des produits de Fortinet
Numéro de Référence	59071012/25
Date de publication	10 Décembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiAnalyzer de 7.2.0 jusqu'à 7.2.5
- FortiAnalyzer de 7.4.0 jusqu'à 7.4.2
- FortiAuthenticator 6.3 toutes les versions
- FortiAuthenticator 6.4 toutes les versions
- FortiAuthenticator 6.5 toutes les versions
- FortiAuthenticator de 6.6.0 jusqu'à 6.6.6
- FortiManager 6.4 toutes les versions
- FortiManager 7.0 toutes les versions
- FortiManager de 7.2.0 jusqu'à 7.2.5
- FortiManager de 7.4.0 jusqu'à 7.4.2
- FortiOS 6.4 toutes les versions
- FortiOS 7.0 toutes les versions
- FortiOS 7.2 toutes les versions
- FortiOS de 7.4.0 jusqu'à 7.4.8
- FortiOS de 7.6.0 jusqu'à 7.6.3
- FortiPortal 6.0 toutes les versions
- FortiProxy de 7.0.0 jusqu'à 7.0.21
- FortiProxy de 7.2.0 jusqu'à 7.2.14
- FortiProxy de 7.4.0 jusqu'à 7.4.10
- FortiProxy de 7.6.0 jusqu'à 7.6.3
- FortiSwitchManager de 7.0.0 jusqu'à 7.0.5
- FortiSwitchManager de 7.2.0 jusqu'à 7.2.6
- FortiWeb de 7.0.0 jusqu'à 7.0.11

- FortiWeb de 7.2.0 jusqu'à 7.2.11
- FortiWeb de 7.4.0 jusqu'à 7.4.10
- FortiWeb de 7.6.0 jusqu'à 7.6.5
- FortiWeb de 8.0.0 jusqu'à 8.0.1
- FortiPAM 1.0 toutes les versions
- FortiPAM 1.1 toutes les versions
- FortiPAM 1.2 toutes les versions
- FortiPAM 1.3 toutes les versions
- FortiPAM 1.4 toutes les versions
- FortiSASE 24.1.b
- FortiSRA 1.4 toutes les versions

Identificateurs externes

CVE-2024-40593 CVE-2024-47570 CVE-2025-57823 CVE-2025-59718 CVE-2025-59719 CVE-2025-59923 CVE-2025-62631 CVE-2025-64447 CVE-2025-64471

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-2025-59718 » et « CVE-2025-59719 » sont critiques. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'élever ses privilèges, de contourner des mesures de sécurité ou d'accéder à des données confidentielles.

Solution

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

Risques

- Exécution de code arbitraire
- Elévation de privilèges
- Contournement de mesures de sécurité
- Accès à des données confidentielles

Références

Bulletins de sécurité de Fortinet:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-133
- https://fortiguard.fortinet.com/psirt/FG-IR-24-268
- https://fortiguard.fortinet.com/psirt/FG-IR-25-411
- https://fortiguard.fortinet.com/psirt/FG-IR-25-554
- https://fortiguard.fortinet.com/psirt/FG-IR-25-616
- https://fortiguard.fortinet.com/psirt/FG-IR-25-647
- https://fortiguard.fortinet.com/psirt/FG-IR-25-945
- https://fortiguard.fortinet.com/psirt/FG-IR-25-984

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma