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	54421405/25
Date de publication	14 Mai 2024
Risque	Critique
Impact	Critique

Systèmes affectés

- FortiOS versions antérieures à la version 7.0.15
- FortiOS versions 7.2.x antérieures à la version 7.2.8
- FortiOS versions 7.4.x antérieures à la version 7.4.7
- FortiOS versions 7.6.x antérieures à la version 7.6.1
- FortiMail versions 7.0.x antérieures à la version 7.0.9
- FortiMail versions 7.2.x antérieures à la version 7.2.8
- FortiMail versions 7.4.x antérieures à la version 7.4.5
- FortiMail versions 7.6.x antérieures à la version 7.6.3
- FortiManager versions 7.0.x antérieures à la version 7.0.8
- FortiManager versions 7.2.x antérieures à la version 7.2.2
- FortiClientMac versions 7.4.x antérieures à la version 7.4.3
- FortiClientMac versions 7.x antérieures à la version 7.2.9
- FortiClientWindows versions 7.2.x antérieures à la version 7.2.2
- FortiNDR versions 7.1.x à 7.2.x antérieures à la version 7.2.5
- FortiNDR versions 7.4.x antérieures à la version 7.4.8
- FortiNDR versions 7.6.x antérieures à la version 7.6.1
- FortiNDR versions antérieures à la version 7.0.7
- FortiPortal versions 7.0.x antérieures à la version 7.0.10
- FortiPortal versions 7.2.x antérieures à la version 7.2.6
- FortiPortal versions 7.4.x antérieures à la version 7.4.2
- FortiProxy versions 7.6.x antérieures à la version 7.6.2
- FortiCamera versions antérieures à la version 2.1.4
- FortiVoice versions 6.4.x antérieures à la version 6.4.11

- FortiVoice versions 7.0.x antérieures à la version 7.0.7
- FortiVoice versions 7.2.x antérieures à la version 7.2.1
- FortiVoiceUCDesktop versions antérieures à la version 7.0
- FortiClientEMS Cloud versions 7.4.x antérieures à la version 7.4.3
- FortiClientEMS versions 7.4.x antérieures à la version 7.4.3
- FortiRecorder versions 6.4.x antérieures à la version 6.4.6
- FortiRecorder versions 7.0.x antérieures à la version 7.0.6
- FortiRecorder versions 7.2.x antérieures à la version 7.2.4
- FortiSwitchManager versions 7.2.x antérieures à la version 7.2.6

Identificateurs externes

CVE-2024-35281 CVE-2024-54020 CVE-2025-22252 CVE-2025-22859 CVE-2025-24473
CVE-2025-25251 CVE-2025-32756 CVE-2025-46777 CVE-2025-47294 CVE-2025-47295

Bilan de la vulnérabilité

Fortinet annonce la disponibilité de mises à jour de sécurité permettant la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder à des informations confidentielles d'élever ses privilèges ou de causer un déni de service.

Une de ces vulnérabilités, identifiée par « CVE-2025-32756 » est critique et activement exploitée.

Solution

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

Risques

- Accès à des données confidentielles
- Exécution de code arbitraire
- Elévation de privilèges
- Déni de service

Références

Bulletins de sécurité de Fortinet:

- https://www.fortiguard.com/psirt/FG-IR-24-023

- https://www.fortiguard.com/psirt/FG-IR-24-025
- https://www.fortiguard.com/psirt/FG-IR-24-380
- https://www.fortiguard.com/psirt/FG-IR-24-381
- https://www.fortiguard.com/psirt/FG-IR-24-388
- https://www.fortiguard.com/psirt/FG-IR-24-472
- https://www.fortiguard.com/psirt/FG-IR-24-548
- https://www.fortiguard.com/psirt/FG-IR-24-552
- https://www.fortiguard.com/psirt/FG-IR-25-016
- https://www.fortiguard.com/psirt/FG-IR-25-254