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	Mises à jour de sécurité pour des produits de Fortinet
Numéro de Référence	46511303/24
Date de publication	13 Mars 2024
Risque	Important
Impact	Important

Systèmes affectés

- FortiClientEMS 7.0 versions antérieures à 7.0.11
- FortiClientEMS 7.2 versions antérieures à 7.2.3
- FortiClientEMS 6.4
- FortiClientEMS 6.2
- FortiClientEMS 6.0
- FortiManager versions antérieures à 7.4.1
- FortiManager versions antérieures à 7.2.4
- FortiManager versions antérieures à 7.0.11
- FortiManager versions antérieures à 6.4.14
- FortiOS 7.4 versions antérieures à 7.4.2
- FortiOS 7.2 versions antérieures à 7.2.6
- FortiOS 7.0 versions antérieures à 7.0.13
- FortiOS 6.4 versions antérieures à 6.4.15
- FortiOS 6.2 versions antérieures à 6.2.16
- FortiProxy 7.4 versions antérieures à 7.4.1
- FortiProxy 7.2 versions antérieures à 7.2.7
- FortiProxy 7.0 versions antérieures à 7.0.13

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

Identificateurs externes

CVE-2023-42789 CVE-2023-42790 CVE-2023-47534 CVE-2024-23112
CVE-2023-36554 CVE-2023-48788

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'injecter du code SQL ou d'accéder à des informations confidentielles.

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
- Injection de code SQL

Références

Bulletins de sécurité de Fortinet:

- https://www.fortiguard.com/psirt/FG-IR-23-390
- https://www.fortiguard.com/psirt/FG-IR-23-328
- https://www.fortiguard.com/psirt/FG-IR-24-013
- https://www.fortiguard.com/psirt/FG-IR-23-103
- https://www.fortiguard.com/psirt/FG-IR-24-007

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