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	41281204/23
Date de publication	12 Avril 2022
Risque	Important
Impact	Critique

Systèmes affectés

- Fortinet FortiSOAR
- Fortinet FortiClientMac
- Fortinet FortiNAC-F
- Fortinet FortiNAC
- Fortinet FortiDDoS-F
- Fortinet FortiDDoS
- Fortinet FortiADC
- Firtinet FortiClientWindows
- Fortient FortiPresence
- Fortinet FortiProxy
- Fortinet FortiOS
- Fortinet FortiAnalyzer
- Fortinet FortiAuthenticator
- Fortinet FortiSIEM
- Fortinet FortiDeceptor
- Fortinet FortiSandbox
- Fortinet FortiManager

Pour plus d'information sur les versions affectées veuillez consulter le bulletin de sécurité de Fortinet

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

Identificateurs externes

CVE-2023-27995	CVE-2023-22635	CVE-2022-43951	CVE-2022-40679
CVE-2022-40682	CVE-2022-42470	CVE-2022-41331	CVE-2022-43948
CVE-2023-22641	CVE-2022-42477	CVE-2022-43952	CVE-2022-43955
CVE-2022-43946	CVE-2022-0847	CVE-2022-27487	CVE-2022-41330
CVE-2022-43947	CVE-2022-27485	CVE-2023-22642	CVE-2022-42469
CVE-2022-35850			

Bilan de la vulnérabilité

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

Solution

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

Risques

- Exécution de code arbitraire à distance
- Elévation de privilèges
- Accès à des informations confidentielles
- Déni de service.
- Contournement de la politique de sécurité

Références

Bulletin de sécurité de Fortinet:

- https://www.fortiguard.com/psirt-monthly-advisory/april-2023-vulnerability-advisories