ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités dans les produits Fortiguard
Numéro de Référence	36750906/22
Date de Publication	09 Juin 2022
Risque	Important
Impact	Important

Systèmes affectés

- FortiAP-U 6.2.4 versions antérieures à 6.2.4
- FortiAuthenticator Agent for Microsoft OWA versions antérieures 2.3
- FortiClientWindows versions 7.0.x antérieures à 7.0.4
- FortiClientWindows versions 6.4.x antérieures à 6.4.8
- FortiDDoS versions antérieures à 5.6.0
- FortiTokenMobile pour Android versions 5.1.x antérieures à 5.1.0
- FortiTokenMobile pour iOS versions 5.3.x antérieures à 5.3.0
- FortiTokenMobile pour Windows versions 4.1.x antérieures à 4.1.0
- FortiOS versions 7.0.x antérieures à 7.0.0
- FortiOS versions 6.4.x antérieures à 6.4.0
- FortiManager versions 7.0.x antérieures à 7.0.2
- FortiManager versions 6.4.x antérieures à 6.4.7
- FortiAnalyzer versions 7.0.x antérieures à 7.0.3
- FortiAnalyzer versions 6.4.x antérieures à 6.4.8
- FortiSandbox versions antérieures à 4.2.0

Identificateurs externes

- CVE-2022-30301 CVE-2022-22304 CVE-2022-26113 CVE-2022-29060 CVE-2021-22131 CVE-2022-22305 CVE-2020-13927 CVE-2020-11982 CVE-2020-11981 CVE-2021-35936 CVE-2021-28359 CVE-2020-13944 CVE-2020-17515 CVE-2021-23336 CVE-2020-17526 CVE-2020-17513

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Bilan de la vulnérabilité

Plusieurs vulnérabilités ont été corrigées dans les produits Fortiguard susmentionnés. Un attaquant pourrait exploiter certaines de ces vulnérabilités pour réussir une élévation de privilèges, provoquer une exécution de code arbitraire à distance, causer un déni de service ou porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Fortiguard du 07 Juin 2022 afin d'installer les nouvelles mises à jour.

Risque

- Elévation des privilèges,
- Exécution du code arbitraire à distance,
- Atteinte à la confidentialité de données ;
- Déni de service,

Annexe

Bulletins de sécurité Fortiguard du 07 Juin 2022:

- https://www.fortiguard.com/psirt-monthly-advisory/june-2022-vulnerability-advisories

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma