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	Zero-Day dans l'antivirus Microsoft Defender
Numéro de Référence	28331301/21
Date de Publication	13 Janvier 2021
Risque	Important
Impact	Important

Systèmes affectés

- Microsoft Malware Protection Engine version antérieure à 1.1.17700.4,

Identificateurs externes

- CVE-2021-1647,

Bilan de la vulnérabilité

Microsoft annonce la correction d'une vulnérabilité de type "zero-day" dans l'antivirus Microsoft Defender. La vulnérabilité a été décrite comme un bug d'exécution de code à distance (RCE) permettant à un attaquant d'exécuter du code sur des appareils vulnérables en incitant un utilisateur à ouvrir un document malveillant sur un système où est installé Microsoft Defender. Il faut noter qu'un exploit de cette vulnérabilité est publiquement disponible, il est fortement recommandé d'installer la nouvelle version de Microsoft Defendre 1.1.17700.4.

Solution

Veuillez vous référer au bulletin de sécurité Microsoft du 12 Janvier 2021**.**

Risque

- Exécution du code arbitraire à distance,

Annexe

Bulletin de sécurité Microsoft du 12 Janvier 2021**:**

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647

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