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

NOTE DE SECURITE

Titre	Microsoft corrige un zéro-day affectant les systèmes Windows exploité dans plusieurs attaques
Numéro de Référence	50851411/24
Date de Publication	14 Novembre 2024
Risque	Critique
Impact	Critique

Une nouvelle vulnérabilité zero-day, « CVE-2024-43451 », a été activement exploitée dans la nature, ciblant les systèmes Windows à travers différentes versions. L'exploit permet à des acteurs malveillants de prendre le contrôle d'un système par un simple clic droit sur un fichier malveillant.

La faille de sécurité « CVE-2024-43451 » est une vulnérabilité de divulgation de hash NTLM par usurpation d'identité, qui peut être exploitée pour voler le hash NTLMv2 de l'utilisateur connecté en le forçant à se connecter à un serveur distant contrôlé par un attaquant. Elle affecte presque toutes les versions de Windows, y compris Windows 10 et 11, ainsi que certaines configurations de versions plus anciennes comme Windows 7 et 8.1.

La vulnérabilité est déclenchée par l'interaction avec des fichiers URL spécialement conçus, présentés comme des documents légitimes, en cliquant avec le bouton droit de la souris, en le supprimant ou en le déplaçant. Une fois que l'utilisateur interagit avec le fichier URL de l'une des manières déclenchantes, une connexion au serveur de l'attaquant est établie, permettant le téléchargement d'un payload malveillant, y compris le malware SparkRAT, un cheval de Troie d'accès à distance open source, utilisé pour prendre le contrôle total du système.

Microsoft a publié un correctif de sécurité le 12 novembre 2024 pour résoudre cette vulnérabilité. Les utilisateurs sont vivement encouragés à mettre à jour leurs systèmes immédiatement afin d'éviter l'exploitation de « CVE-2024-43451 ».

Référence:

- Bulletin de sécurité maCERT du 13 Novembre 2024 :
- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilites-critiques-dans-microsoft-windows-patch-tuesday-novembre-2024
- https://www.kaspersky.com/blog/2024-november-patch-tuesday/52604/