AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre de Réponse aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

Le Bloc-notes de Windows 11 permet l'exécution de fichiers malveillants

Contenu

I. Introduction 3
II. Contexte 3
III. Détails techniques de la vulnérabilité 3
IV. Mesures de remédiation et correctifs 3
V. Conclusion 4
VI. Annexes 5

I. Introduction

Longtemps resté un éditeur de texte brut minimaliste, le Bloc-notes (Notepad) de Windows 11 a récemment bénéficié d'une refonte majeure incluant le support du format Markdown. Cependant, cette modernisation a introduit une vulnérabilité critique de type exécution de code à distance (RCE), permettant à des attaquants de lancer des programmes malveillants sans aucun avertissement de sécurité.

II. Contexte

Cette vulnérabilité survient alors que Microsoft a supprimé WordPad de Windows 11, positionnant le Bloc-notes comme le remplaçant hybride entre éditeur de texte simple et éditeur de texte enrichi (RTF). L'ajout de fonctionnalités complexes dans des outils historiquement "légers" augmente mécaniquement la surface d'attaque, comme l'illustre cette capacité à lancer des protocoles non vérifiés

III. Détails techniques de la vulnérabilité

La faille, identifiée sous la référence **CVE-2026-20841**, repose sur une neutralisation incorrecte des éléments spéciaux lors de l'interprétation des commandes (injection de commande).

Dans les **versions 11.2510** et antérieures du Bloc-notes, l'application gérait mal certains protocoles URI au sein des fichiers .md. En exploitant le mode de prévisualisation Markdown, un attaquant pouvait dissimuler des liens malveillants qui, une fois activés, contournaient les mécanismes de défense habituels de Windows.

Détails techniques de l'exploitation :

- **Vecteur :** Un fichier Markdown (.md) spécialement conçu.
- **Mécanisme :** Utilisation de liens pointant vers des fichiers locaux ou distants via les protocoles file://, ms-appinstaller://, ou des partages SMB.
- **Action utilisateur :** Un simple Ctrl + Clic sur le lien déclenchait l'exécution immédiate.
- **Privilèges :** Le code malveillant s'exécutait avec les mêmes droits que l'utilisateur local.

IV. Mesures de remédiation et correctifs

Microsoft a déployé un correctif dont les tests de sécurité confirment que le comportement de l'application a été modifié :

1. **Validation des protocoles** : Seuls les liens http:// et https:// sont désormais considérés comme sûrs.
2. **Alertes de sécurité** : Pour tout autre type de lien (file:, ms-settings:, mailto:, etc.), le Bloc-notes affiche désormais systématiquement une boîte de dialogue d'avertissement avant toute exécution.
3. **Mise à jour automatique** : Le correctif est diffusé via le Microsoft Store, limitant ainsi la durée d'exposition pour la majorité des utilisateurs.

V. Conclusion

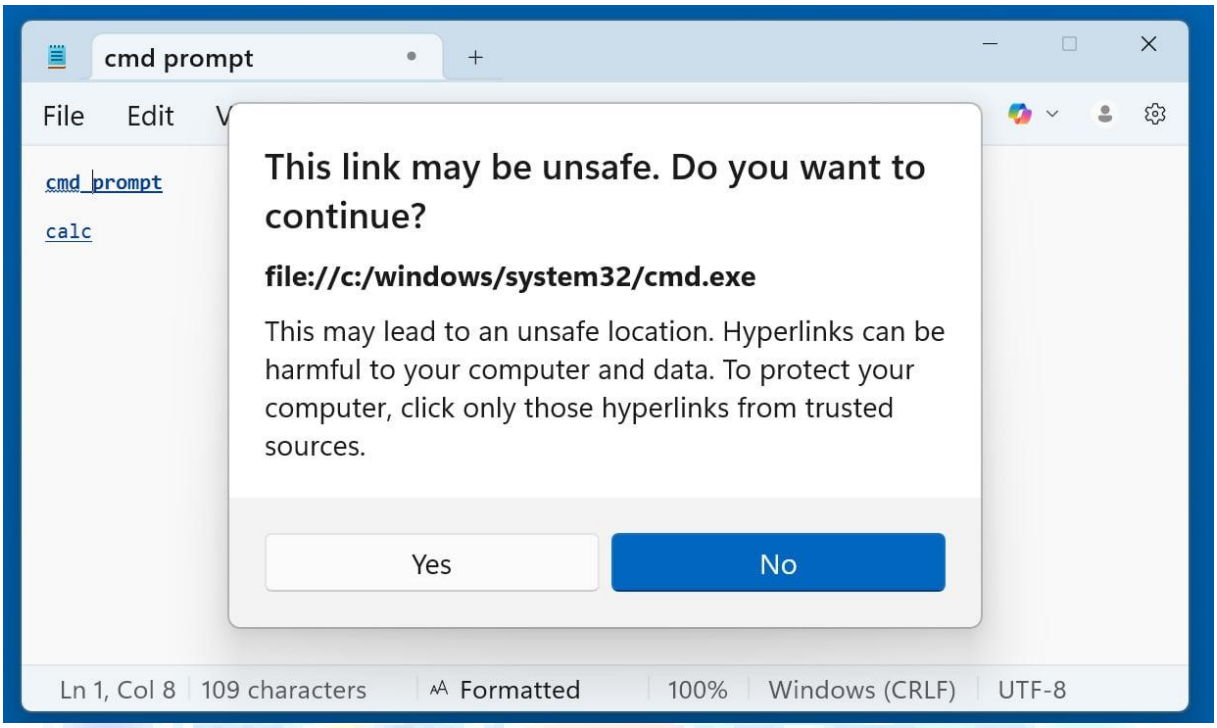
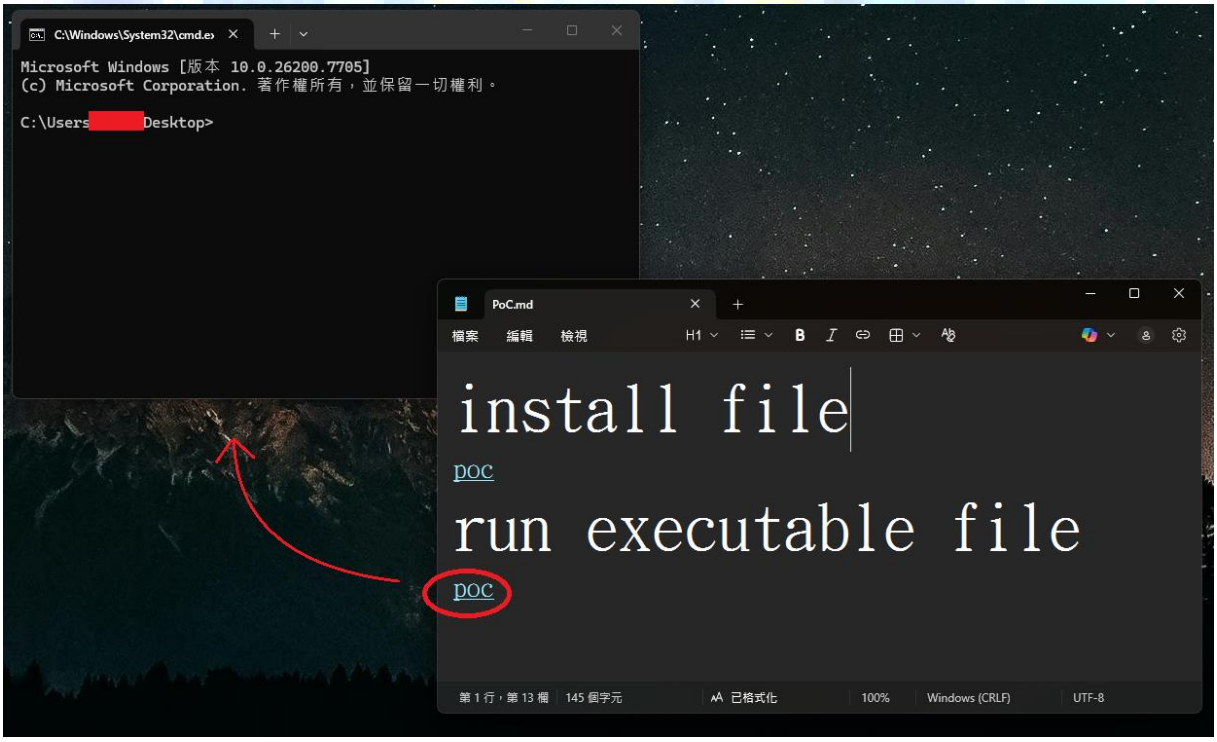
Bien que l'alerte soit désormais présente, le risque d'ingénierie sociale subsiste si un utilisateur est incité à cliquer sur "Oui". La vigilance reste de mise lors de l'ouverture de fichiers Markdown de sources inconnues.

Néanmoins, pour éviter d'être victime d'un acteur malveillant connu ou non, il est recommandé de prendre les précautions suivantes :

- N'installer que les applications qui vous sont utiles ;
- Se rassurer de la crédibilité d'une application à l'aide des notes et commentaires attribués par les utilisateurs à celle-ci, avant de les installer ;
- Installer les applications depuis le Store officiel de votre Système d'exploitation (Play Store pour Google Android, App Store pour IOS, etc.) ;
- N'accordez que les autorisations utiles à vos applications pour réaliser les fonctions qu'elles sont censées réaliser ;
- Veillez à mettre à jour régulièrement tous vos logiciels, en installant chaque nouveau correctif de sécurité dès sa publication ;
- Choisissez une solution de sécurité (Antivirus) éprouvée dotée de capacités de détection comportementale pour une protection efficace contre les menaces connues et inconnues, notamment les exploitations de vulnérabilités ;
- Armez-vous des règles élémentaires de cyber-hygiène.

VI. Annexes

Les alertes Windows concernant les liens suspects



Une commande lancée sans avertissement