CYBER DEFENSE AFRICA : ANNONCE DE SÉCURITÉ **Date** : 05/09/2024

Type de Contenu	Description
Titre	***Exploitation en cours de la vulnérabilité 0-Day Windows Kernel Privilege Escalation (escalade des privilèges du noyau Windows) - CVE-2024-38106***
ID	*202409/AS/23*
Code TLP	*Green*
Niveau de Risque	***Elevé***
Application et service affectés	***Windows et Windows Server***
Version / Edition	*Windows 10, 11 et Windows Server (2016, 2019, 2022)*
Plateforme	***N/A***
Mise à jour	*Appliquer les correctifs nécessaires aux produits vulnérables pour éviter qu'ils ne soient exploités.*
Résumé	*Exploitation active de la vulnérabilité 0-Day Windows Kernel Privilege Escalation (CVE-2024-38106)*
Impacts	- ***Obtention des privilèges de niveau SYSTÈME sur le système affecté*** - ***Création de comptes cachés*** - ***Exfiltration de données sensibles*** - ***Chiffrement de données et effacement des logs*** - ***Modification des configurations de sécurité et Installation de logiciels malveillants***
Description Détaillée	*Microsoft a publié plusieurs correctifs pour de multiples vulnérabilités lors du Patch Tuesday du mois d'août 2024. L'une des vulnérabilités répertoriées par Microsoft est la* ***CVE-2024-38106****.* *Cette vulnérabilité est associée à l'escalade des privilèges du noyau Windows et affecte plusieurs systèmes d'exploitation Microsoft Windows, notamment* ***Windows 10, 11 et Windows Server (2016, 2019, 2022)****.* *En effet, Microsoft a déclaré que cette vulnérabilité était activement exploitée par des groupes de cyberattaques.* *En pratique, Microsoft a également mentionné qu'aucune interaction de l'utilisateur n'était nécessaire pour exploiter cette vulnérabilité.* *La gravité de cette vulnérabilité est de 7.0 (élevée).*
Recommandations	***Les organisations doivent appliquer les correctifs nécessaires aux produits vulnérables pour éviter qu'ils ne soient exploités.***
Indicateurs de Compromission	*N/A*
Liens pour plus de détails	*https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38106*