DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 11-12-2024

BULLETIN ALERTES

Object	Vulnérabilité zero-day dans Windows
Réference	1291
Date de Publication	2024-12-11
Sévérité	Critique

IMPACT :

- Perte d'intégrité
- Perte de confidentialité

SYSTÉME AFFECTÉ :

- Windows 7
- Server 2008 R2 jusqu'à Windows11 24H2
- Server 2022

DÉSCRIPTION :

Une vulnérabilité zero-day a été découverte, permettant à un attaquant de capturer des identifiants NTLM en incitant une cible à visualiser un fichier malveillant dans l'Explorateur Windows.

SOLUTION :

Activer l'Extended Protection for Authentication(EPA) sur les services LDAP, AD CS, Exchange

DOCUMENTATION :

https://www.tomshardware.com/tech-industry/cyber-security/zero-day-windows-ntlm-hash-vulnerability-gets-patched-by-third-party-credentials-can-be-hijacked-by-merely-viewing-a-malicious-file-in-file-explorer

https://www.darkreading.com/application-security/microsoft-ntlm-zero-day-remain-unpatched-april