**ROYAUME DU MAROC**
**ADMINISTRATION**
**DE LA DEFENSE NATIONALE**
**Direction Générale de la Sécurité des Systèmes d'Information**
**Centre de Veille de Détection et de Réaction aux Attaques Informatiques**

**المملكة المغربية**
**إدارة الدفاع الوطني**
**المديرية العامة لأمن نظم المعلومات**
**مركز اليقظة والرصد والتصدي للهجمات المعلوماتية**

**NOTE DE SECURITE**

| | |
|---|---|
| **Titre** | Zero-day « BlueHammer » affectant Windows |
| **Numéro de Référence** | 62990904/26 |
| **Date de publication** | 09 avril 2026 |

Un chercheur en sécurité, connu sous les pseudonymes « Chaotic Eclipse » ou « Nightmare-Eclipse », a publié publiquement le code d'exploit d'une vulnérabilité de type élévation de privilèges locale sur Windows nommée « BlueHammer ».

Cette publication intervient en réaction à une gestion jugée insatisfaisante de sa divulgation par le Microsoft Security Response Center (MSRC), et constitue donc une divulgation non coordonnée d'un zero-day.

BlueHammer exploite une vulnérabilité liée au mécanisme de mise à jour des signatures de Windows Defender et impacte tous les systèmes Windows quand Windows Defender est actif. Elle permet à un attaquant déjà présent sur la machine avec un compte utilisateur standard d'obtenir des privilèges SYSTEM et d'accéder à la base de données SAM, contenant les hashes de mots de passe locaux.

## Mesures de mitigation

À ce jour, aucun correctif officiel n'est encore disponible. Il est cependant recommandé de :

- Appliquer des règles AppLocker/WDAC ou politiques de restriction des binaires non signés
- Mettre en place des règles de détection autour des accès inhabituels à SAM ou aux dossiers

de définitions

- Limiter les écritures dans les répertoires sensibles et surveiller les modifications dans les chemins liés à Defender
- Surveiller les événements de création de processus avec token SYSTEM inhabituels (via EDR/XDR si disponible)

## Références

L'exploit de la vulnérabilité publié sur Github :

- https://github.com/Nightmare-Eclipse/BlueHammer?tab=readme-ov-file