**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 D'INFORMATION

| | |
|---|---|
| **Titre** | Microsoft corrige un Zero-day exploité par le RAT "MysterySnail" |
| **Numéro de Référence** | 32731310/21 |
| **Date de Publication** | 13 Octobre 2021 |
| **Risque** | Critique |
| **Impact** | Critique |

Un nouveau cheval de Troie d'accès à distance (RAT), nommé "MysterySnail", a été observé exploitant une vulnérabilité de type "zero-day", suivie par "CVE-2021-40449".

La vulnérabilité est une faille de type "use-after-free" dans la fonction "NtGdiResetDC" de "Win32k" qui pourrait permettre à un attaquant de réussir une élévation de privilèges et d'exécuter des fonctions API inattendues. Le RAT MysterySnail est conçu pour collecter et exfiltrer les informations système des hôtes compromis avant d'atteindre le serveur de commande et de contrôle (C2) pour d'autres commandes.

Microsoft a corrigé cette critique faille dans son patch Tuesday du mois Octobre 2021. Il est fortement recommandé d'appliquer immédiatement les correctifs nécessaires pour éviter toutes tentatives de compromission.

## Indices de compromission :

- www[.]disktest[.]com
- www[.]runblerx[.]com
- http[.]ddspadus[.]com

- MD5: e2f2d2832da0facbd716d6ad298073ca
- SHA1: ecdec44d3ce31532d9831b139ea04bf48cde9090
- SHA256: b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

## Annexe

Bulletin de sécurité Microsoft du 12 Octobre 2021**:**

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-40449
- https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma