Agence Nationale
des Systémes d'information
de l'état

Djibouti le, 03-07-2023

BULLETIN ALERTES

Object	Vulnérabilité dans Microsoft Outlook
Réference	1034
Date de Publication	2023-03-29
Sévérité	Critique

IMPACT :

- Élévation de privilèges
- Pertes d'intégrité
- Atteinte à la confidentialité des données

SYSTÉME AFFECTÉ :

- Microsoft Outlook 2013 RT Service Pack 1
- Microsoft Outlook 2013 Service Pack 1 (éditions 32 bits)
- Microsoft Outlook 2013 Service Pack 1 (éditions 64 bits)
- Microsoft Outlook 2016 (édition 32 bits)
- Microsoft Outlook 2016 (édition 64 bits)

DÉSCRIPTION :

Microsoft a publié l'existence d'une vulnérabilité critique CVE-2023-23397 dans le produit Microsoft Outlook permettant une élévation de privilèges à un attaquant distant. Cette vulnérabilité ne nécessite pas une intervention de l'utilisateur et peut-être exploite en envoyant un e-mail malveillant contenant un lien UNV lorsqu'il est récupéré et traité par le client Outlook, force la cible à s'authentifier auprès d'un serveur contrôlé par l'attaquant. Pendant l'authentification vers le serveur malveillant le message de négociation NTLM de l'utilisateur est envoyé donc l'attaquant peut ensuite relayer l'authentification vers d'autres systèmes qui prennent en charge l'authentification NTLM . L'exploit de la vulnérabilité peut se produire avant que l'e-mail ne soit affiché dans le volet de prévisualisation.

Microsoft a fourni un script PowerShell pour l'identification de compromission. Ce script vérifie si une propriété est renseignée avec une valeur de chaîne non vide dans les éléments de messagerie Exchange (courrier, calendrier et tâches) afin de déterminer si la valeur est malveillante ou non.

SOLUTION :

Mettre à jour les produits Microsoft Outlook.(se réfère à la documentation)

DOCUMENTATION :

- Bulletin de sécurité Microsoft CVE-2023-23397 du 14-03-2023
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-23397
- code Powershell f
  https://aka.ms/CVE-2023-23397ScriptDoc
- CVE-2023-23397
  https://www.cve.org/CVERecord?id=CVE-2023-23397