



BULLETIN DE SECURITE

Titre	Zero-day affectant les systems Windows
Numéro de Référence	3347241121
Date de Publication	24 Novembre 2021
Risque	Important
Impact	Important

Systemes affectés

- Windows 10, 11
- Windows Server 2022

Identificateurs externes

- CVE-2021-41379

Bilan de la vulnérabilité

Dans le cadre du Patch Tuesday de novembre 2021, Microsoft a corrigé une vulnérabilité de type "Windows Installer Elevation of Privilege Vulnerability" suivit par « CVE-2021-41379 ». Un chercheur en sécurité a identifié un contournement du correctif et a divulgué publiquement un exploit pour cette vulnérabilité permettant l'élévation de privilèges sur les systèmes Windows 10, 11 et Windows Server 2022. Un attaquant ayant un accès limité à une machine peut utiliser cet exploit et élever ses privilèges pour avoir des privilèges "SYSTEM".

Solution

Aucun correctif de sécurité n'est disponible pour le moment. Il est fortement recommandé de surveiller l'activité des systèmes concernés pour détecter et investiguer toutes les tentatives d'élévation de privilèges.

Risque

- Elévation de privilèges,

Annexe

- <https://www.bleepingcomputer.com/news/microsoft/new-windows-zero-day-with-public-exploit-lets-you-become-an-admin/>