DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Exploatarea unei vulnerabilități Microsoft de tip zero-day poate oferi atacatorilor drepturi de administrare în Windows

Un cercetător de securitate a dezvăluit public un exploit pentru o nouă vulnerabilitate zero-day 'local privilege elevation' pentru Windows, care oferă privilegii de administrare în Windows 10, Windows 11 și Windows Server.

Folosind această vulnerabilitate, un atacator care are acces limitat la un dispozitiv compromis își poate spori cu ușurință privilegiile pentru a ajuta la răspândirea laterală în cadrul rețelei.

Vulnerabilitatea afectează toate versiunile acceptate de Windows, inclusiv Windows 10, Windows 11 și Windows Server 2022.

Ca parte a November 2021 Patch Tuesday, Microsoft a rezolvat o vulnerabilitate „Windows Installer Elevation of Privilege Vulnerability" (CVE-2021-41379). Aceasta fusese descoperită de cercetătorul de securitate Abdelhamid Naceri. După ce a analizat soluția Microsoft de a rezolva această vulnerabilitate, Naceri a găsit o nouă metodă de a eluda patch-ul de securitate, dar și o nouă vulnerabiltate zero-day de elevare a privilegiilor, de această dată una și mai critică decât precedenta.

Recent, cercetătorul a publicat un exploit de tip Proof of Concept pentru acest nou zero-day pe GitHub, explicând că funcționează pe toate versiunile acceptate de Windows.

https://vimeo.com/648758294

Publicația online BleepingComputer a testat acest exploit realizat de Naceri – InstallerFileTakeOver - și a observat că durează doar câteva secunde pentru a obține privilegii de sistem dintr-un cont de test cu privilegii standard.

Microsoft a oferit un punct de vedere referitor la această nouă descoperire: „Suntem conștienți de noua dezvăluire și vom face tot ceea ce este necesar pentru a menține clienții noștri în siguranță și protejați. Un atacator care utilizează metodele descrise trebuie să aibă deja acces, dar și capacitatea de a rula codul pe mașina unei victime țintă."

Cel mai probabil Microsoft va adresa această nouă vulnerabiltate printr-un alt patch de securitate.

Cu toate acestea, Naceri a avertizat că nu este recomandat pentru companiile terțe să încerce să repare vulnerabilitatea: „Cea mai bună soluție disponibilă la momentul scrierii este să aștepte ca Microsoft să elibereze un patch de securitate, din cauza complexității acestei vulnerabilități".

În altă ordine de idei, Cisco Talos a adresat această problemă de securitate prin lansarea unor noi reguli de protecție împotriva exploatării acestei vulnetabilități în Microsoft Windows Installer. Acestea sunt disponibile aici: https://snort.org/advisories/talos-rules-2021-11-23

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

https://blog.talosintelligence.com/2021/11/attackers-exploiting-zero-day.html