AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

CVE-2020-0796 SMBv3 Vulnerability

06/04/2020

Autoriteti Kombetar per Certifikim Eletronik dhe Sigurine Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Përshkrimi i problemit

CVE-2020-0796 është një vulnerabilitet i ekzekutimit të kodit në distancë që prek serverin e bllokut të mesazhit të Microsoft me version 3.1.1 (SMBv3). Dobësia është shkaktuar nga një mbingarkesë në një funksion dekompresimi të driverit të kernelit srv2.sys, i cili është përgjegjës për përpunimin e paketave SMB.

Një sulmues i paautorizuar mund ta shfrytëzojë këtë vulnerabilitet duke i dërguar serverit SMB një paketë të krijuar posaçërisht për këtë sulm. Për më tepër, klientët e tjere SMB që lidhen me serverët e kompromentuar SMB, janë gjithashtu vulnerabel.

Vulnerabiliteti afekton këto versione:

- Windows 10 Version 1903 for 32-bit Systems
- Windows 10 Version 1903 for ARM64-based Systems
- Windows 10 Version 1903 for x64-based Systems
- Windows 10 Version 1909 for 32-bit Systems
- Windows 10 Version 1909 for ARM64-based Systems
- Windows 10 Version 1909 for x64-based Systems
- Windows Server, version 1903 (Server Core installation)
- Windows Server, version 1909 (Server Core installation)

Zgjidhja e problemit

Microsoft rekomandon aplikimin e rrugës së mëposhtme për të parandaluar shfrytëzimin e ketij vulnerabiliteti në serverat SMB:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 -Force
```

Për më tepër, rekomandohet bllokimi i portes TCP 445 në perimetrin e rrjetit në mënyrë që të mbrohen sistemet nga sulmet me origjinë nga jashtë.

Gjithashtu së fundmi Microsoft ka lëshuar një azhurnim për të rregulluar këtë vulnerabilitet (KB4551762) të cilin e gjeni tek linku i mëposhtëm:

https://support.microsoft.com/en-us/help/4551762/windows-10-update-kb4551762

Masat të tjera për këtë vulnerabilitet përfshijnë:

- Bllokimin e lidhjeve SMB që kanë kontakt direct me nderfaqet e internetit
- Caktivizimin e kompresimit te SMBv3 nga ana e serverit

Referenca

a) https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0796
b) https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200005