Raport consolidat eveniment cibernetic

CVE-2024-38145

CVE-2024-38145 este o vulnerabilitate care afectează *Windows Layer-2 Bridge Network Driver*. Această vulnerabilitate facilitează desfășurarea unor acțiuni malițioase de tip DoS orientate către indisponibilizarea driver-ului de rețea.

Informații suplimentare

TIP	CVE-2024-38145
Versiunile Afectate	• Windows 10 (versiuni 1507, 1607, 1809, 21H2, 22H2). • Windows 11 (versiuni 21H2, 22H2, 23H2, 24H2). • Windows Server (2012, 2012 R2, 2016, 2019, 2022).
Condițiile de exploatare	• Prezența unui sistem cu driver vulnerabil. • Driver *Layer-2 Bridge* este activ, ce permite atacatorului să expedieze pachetele malformate. • Posibilitatea procesării a pachetelor malformate care determină **NULL Pointer Dereference** în driver. • Atacatorul trebuie să aibă acces la rețea pentru a expedia pachetele.
Instrumente de analiză	• Scanarea sistemelor cu instrumente precum: *Nessus, Qualys, OpenVas.* • Analiza traficului: Wireshark • Capturarea traficului din linia de comandă: "**sudo tcpdump -i eth0 port 67 or port 68 -w dhcp_traffic.pcap**" • Implementarea a sistemelor de monitorizare a traficului rețelei cum ar fi *Zabbix, Nagios, PRTG, Observium.* • Implementarea a soluțiilor de management a evenimentelor și informațiilor de securitate (SIEM), ce permit colectarea și analiza traficului de rețea pentru a detecta și colera evenimentele suspecte. • Folosirea instrumentelor de management al patch-urilor pe serverele *Windows* cum ar fi *SCCM* și *WSUS.* • Utilizarea *PowerShell*-ului pentru verificarea Patch-urilor instalate. Pentru verificarea a toate patch-urile folosim comanda: **"Get-HotFix | Sort-Object InstalledOn -Descending"** Pentru căutarea unui patch specific folosim comanda: **"Get-HotFix -Id KB5041782"** • Utilizarea *WMIC*, accesăm linia de comandă și introducem: **"wmic qfe list brief /format:table"**

	• Verificăm în *Registry Editor* lista de patch-uri instalate: **“HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Component Based Servicing\Packages”**
Recomandări generice	• Aplicarea de Patch-uri: se recomandă aplicarea imediată a patch-urilor pentru toate versiunile afectate, furnizate de Microsoft cum ar fi: Windows 10: KB5041782, KB5041773, KB5041578. Windows 11: KB5041592, KB5041585. Windows Server: KB5041851, KB5041828, KB5041573. • Segmentarea rețelei critice și a celor expuse pentru a minimiza impactul. • Configurarea Firewall pentru restricționarea accesului la porturile vulnerabile și implementarea regulilor stricte de firewall

Resurse externe

https://windowsforum.com/threads/cve-2024-38145-critical-windows-vulnerability-in-layer-2-bridge-driver.341835/
https://www.rapid7.com/blog/post/2024/08/13/patch-tuesday-august-2024/
https://www.rapid7.com/db/vulnerabilities/msft-cve-2024-38145/