



Raport consolidat eveniment cibernetic

CVE-2024-38140

CVE-2024-38140 este o vulnerabilitate critică clasificată ca *Remote Code Execution (RCE)* în *Windows Reliable Multicast Transport (RMCAST) Driver*. Aceasta permite atacatorilor să execute cod arbitrar pe sistemele afectate fără a necesita autentificare sau interacțiune din partea utilizatorului.

Componenta afectată: driver-ul *RMCAST* utilizat de **SO Windows** pentru gestionarea comunicării multicast pe rețea.

Tip Vulnerabilitate este clasificată ca o problemă de tip *Use-After-Free* (CWE-416), aceasta se întâmplă atunci când programul gestionează incorect memoria și continuă să utilizeze o locație de memorie după ce aceasta a fost eliberată.

Vectorul de Atac: Vulnerabilitatea poate fi exploatată de la distanță prin rețea. Atacatorul transmite pachete prin intermediul la o rețea special creată către un sistem vulnerabil.

Utilizarea: Poate fi parte componentă a unor atacuri complexe în campanii avansate de tip *APT* (*Advanced Persistent Threat*) pentru a obține persistență pe termeni mai lungi.

Informații suplimentare

TIP	CVE Exploatat
Instrumente pentru analiză	• Scanarea sistemelor cu Vulnerability Scanners cum ar fi <i>Nessus</i>, <i>Qualys</i>, <i>Rapid7 InsightVM</i> sau <i>OpenVas</i>. • Executarea scan de conformitate pentru a verifica daca versiunea patch-urilor este la ZI prin comanda: “nessus -q -x <target_ip> -p CVE-2024-38140”. • Verificarea manuală a versiunii Driver-ului cu ajutorul la PowerShell cu comanda: “Get-WmiObject Win32_PnPSignedDriver Where-Object {\$_.DeviceName -like "*RMCAST*"} Select-Object DeviceName, DriverVersion” • Analiza Event Logs pentru detectarea a activităților suspecte legate de procesul <i>rmcast.sys</i>; comanda pentru PowerShell: “Get-EventLog -LogName System Where-Object {\$_.Source -eq "RMCAST"}” • Compararea a Hash-urilor Driver-ului pentru fișierul <i>rmcast.sys</i> “certutil -hashfile C:\Windows\System32\drivers\rmcast.sys SHA256”
Condiții de exploatare	Disponibilitate la rețeaua în care se află dispozitivul vulnerabil pentru expedierea pachetelor, inclusiv prin lipsă unui proces de autentificare, ceea ce permite atacatorului să lanseze atacul fără a avea nevoie de acreditări valide sau fără ca utilizatorul să efectueze acțiuni.
Impact	Exploatarea vulnerabilității ar putea duce la prelucrarea completă a sistemului, permițând executarea oricărui cod malițios.
Recomandări generice	• Aplicarea Patch-urilor: Instalarea patch-ul de securitate furnizat de Microsoft pentru a atenua aceeaș incident. • Segmentarea Rețelei și Configurarea Firewall: Restricționarea accesului rețelei la sistemele care rulează driver-ul <i>RMCAST</i> și implementarea regurilor stricte de firewall pentru a limita potențialele atacuri.

Resurse externe



<https://windowsforum.com/threads/cve-2024-38140-explained-windows-rmcast-rce-vulnerability-overview.341830/>