



Raport consolidat eveniment cibernetic

CVE-2024-38063

- **CVE-2024-38063** este o vulnerabilitate **zero-click** ce utilizează pachete special concepute pentru a executa un cod arbitrar pe sistemele Windows 10, Windows 11 și Windows Server folosind protocoalele de rețea **Ipv6**.
- Este cauzat de un defect **Integer Underflow**
- Vulnerabilitatea provine din modul în care **TCP/IP** procesează pachetele **IPv6**, creând o cale prin care atacatorii pot exploata sistemul.
- **CVE-2024-38063** este una dintre cele mai grave vulnerabilități remediate de Microsoft, etichetând-o drept un defect **wormable**.

Informații sumare

TIP	CVE-2024-38063 Zero-click Windows TCP/IP
Instrumente pentru analiză	<ul style="list-style-type: none">● Pentru scanarea rețelei – Wireshark, TCPDUMP, Angry IP Scanner● Anliză și detectare -Sysmon , Procces Hacker
Aspecte tehnice	<ul style="list-style-type: none">● Condiții de exploatare: Vulnerabilitatea necesită activarea IPv6 pe sistemul afectat. Dacă IPv6 nu este utilizat, riscul de exploatare dispare.● Vector de atac: Un atacator trimite pachete IPv6 special concepute către sistemul țintă, declanșând vulnerabilitatea.● Impact: Dacă vulnerabilitatea este exploatat cu succes, atacatorul poate executa codul arbitrar pe mașina țintă. Acest lucru ar putea duce la compromiterea completă al sistemului.
Etapele de exploatare	<ol style="list-style-type: none">1. Inițierea exploatării: atacatorul trimite pachete IPv6 rău intenționate către un sistem Windows țintă.2. Declanșator de vulnerabilitate: din cauza manipulării necorespunzătoare a acestor pachete, răspunsul sistemului poate duce la executarea unui cod arbitrar.3. Execuție de la distanță: atacatorul obține controlul asupra sistemului afectat, putând: compromite datele sensibile, întrerupe operațiunile sistemului, efectuarea acțiunilor neautorizate sau instalarea unui soft rău intenționat
Recomandări generice	<ol style="list-style-type: none">1. Dezactivați IPv6: dacă IPv6 nu este necesar pentru mediul dvs., luați în considerare dezactivarea acestuia.2. Monitorizare și răspuns: implementați soluții de monitorizare pentru a detecta traficul IPv6 neobișnuit sau neautorizat. Un sistem de monitorizare eficient poate ajuta la identificarea și răspunsul la potențialele exploatări.3. Actualizarea sistemelor: Asigurați-vă că sistemele dvs. Windows sunt actualizate cu cele mai recente actualizări de securitate și corecții.

Resurse externe



<https://www.bleepingcomputer.com/news/microsoft/zero-click-windows-tcp-ip-rce-impacts-all-systems-with-ipv6-enabled-patch-now/>



<https://securityboulevard.com/2024/08/cve-2024-38063-an-in-depth-look-at-the-critical-remote-code-execution-vulnerability/>