Top Vulnerabilități Critice 2024 pentru Windows

În anul 2024, Microsoft a identificat și remediat numeroase vulnerabilități critice atât sistemul său de operare cât și în diverse aplicați asociate. Prezentul raport listează top *25 de vulnerabilități critice*, oferind o atenție sporită tipurilor de activități malițioase precum *executarea de cod la distanță (RCE), escaladarea privilegiilor (EoP) și ocolirea măsurilor de securitate.*

COD	DESCRIERE	VERSIUNI AFECTATE
CVE-2024-49075	RCE în Windows Remote Desktop Services prin pachete RDP manipulate.	Windows Server 2022, 2019, 10
CVE-2024-49084	Vulnerabilitate în Kernel permite escaladarea privilegiilor.	Windows 11, Windows 10
CVE-2024-49096	RCE în Windows Message Queuing permite control la distanță asupra sistemului.	Windows Server, Windows 11
CVE-2024-49105	RCE în Remote Desktop Client la deschiderea fișierelor RDP malițioase.	Windows 11, 10
CVE-2024-49119	Ocolirea Secure Boot permite inițializarea unui bootloader malițios.	Windows Server 2019, 10
CVE-2024-49135	RCE prin DirectX exploatat folosind fișiere media corupte.	Windows 10, 11
CVE-2024-49122	Vulnerabilitate RPC expune informații sensibile.	Windows Server 2016, 2019
CVE-2024-49128	Ocolire protecție în Microsoft Defender pentru bypass antivirus.	Windows Server 2022, Windows 10
CVE-2024-49131	CSRF în Remote Assistance permite atacuri man-in-the-middle.	Windows 10, 11
CVE-2024-49108	Vulnerabilitate HTTP.sys permite atacuri de tip denial-of-service.	Windows Server 2022
CVE-2024-49126	Dezvăluirea informațiilor prin LSASS expune date despre utilizatori autentificați.	Windows Server, Windows 11
CVE-2024-49138	RCE prin Windows Kernel-Mode Drivers.	Windows 10, Windows 11
CVE-2024-49115	Escaladare de privilegii prin vulnerabilități Kernel.	Windows 10, 11
CVE-2024-49093	Vulnerabilitate ReFS permite coruperea fișierelor critice.	Windows Server 2019, 2022
CVE-2024-49082	RCE în Windows File Explorer prin fișiere corupte.	Windows 10, Windows 11

CVE-2024-49085	DoS în Routing and Remote Access Service (RRAS).	Windows Server 2019
CVE-2024-49101	Vulnerabilitate SMB permite execuția codului malițios pe servere expuse.	Windows Server 2022, 2016
CVE-2024-49072	Vulnerabilitate Task Scheduler permite execuția codului la nivel local.	Windows 10, 11
CVE-2024-49132	Probleme în RDP permit atacuri de tip **RCE**.	Windows Server 2016, 2019
CVE-2024-49114	DoS în rolul DNS Server afectează disponibilitatea serviciilor.	Windows Server 2022, 2019
CVE-2024-49110	Ocolire protecție în autentificarea Windows Hello.	Windows 10, 11
CVE-2024-49078	Executarea neautorizată de comenzi în PowerShell.	Windows 10, Windows 11
CVE-2024-49150	Vulnerabilitate Kernel permite **Privilege Escalation** prin componente GDI.	Windows Server, Windows 11
CVE-2024-49089	Race Condition permite acces neautorizat la resurse partajate.	Windows Server, Windows 11
CVE-2024-49145	Probleme în procesarea fișierelor XML duc la atacuri XXE.	Windows Server, Windows 10

TOP 5 VULNERABILITĂȚI CRITICE CVE

CVE-2024-49075

Metode de exploatare
- Atacatorul scanează serviciile **RDP** expuse folosind **Shodan** sau **Nmap;**
- Exploatează această vulnerabilitate folosind un exploit kit pentru RDP.

Aspecte critice
- Permite atacatorilor să obțină acces complet asupra serverului vulnerabil;
- Exploatarea nu necesită autentificare.

Măsuri de remediere
- Aplicarea imediată a patch-urilor oferite de Microsoft (KB5029699);
- Restricționarea accesului RDP prin firewall și configurarea **Network Level Authentication (NLA)**;
- Implementarea autentificării multi-factor (MFA) pentru acces RDP.

CVE-2024-49084

Metode de exploatare
- Atacatorul folosește un exploit local pentru Kernel pentru a accesa memoria privilegiată;
- Codul exploatabil este injectat în procesele sistemului.

	Aspecte critice • Permite unui utilizator cu privilegii reduse să escaladeze drepturile la nivel **SYSTEM**; • Esențial pentru persistență în atacuri avansate. **Măsuri de remediere**: • Aplicarea patch-urilor lunare (ex. KB5029711); • Monitorizarea atentă a proceselor privilegiate folosind **Sysmon**; • Restricționarea drepturilor pentru utilizatorii neesențiali.
CVE-2024-49119	**Metode de exploatare** • Modificarea firmware-ului pentru a încărca bootloader neautorizat; • Exploatarea atacurilor fizice sau prin dispozitive infectate; **Aspecte critice** • Compromite integritatea sistemului înainte ca sistemul de operare să pornească; • Persistență dificil de detectat. **Măsuri de remediere** • Aplicarea patch-urilor UEFI/BIOS furnizate de producător; • Activarea **BitLocker** pentru protecția împotriva accesului neautorizat; • Audit regulat al configurațiilor **Secure Boot**.
CVE-2024-49105	**Metode de exploatare** • Atacatorul trimite un fișier **RDP** prin e-mail sau descărcare compromisă; • Exploatarea are loc când utilizatorul deschide fișierul fără precauții. **Aspecte critice** • Exploatarea necesită interacțiunea utilizatorului; • Poate fi utilizată în atacuri de tip **phishing** sau **social engineering**. **Măsuri de remediere** • Aplicarea patch-urilor de securitate de la Microsoft; • Blocarea fișierelor **.rdp** provenite din surse necunoscute; ▪ Utilizarea soluțiilor de securitate endpoint pentru scanarea fișierelor.

CVE-2024-49135	**Metode de exploatare** • Atacatorul creează un fișier video sau grafic special modificat; • Fișierul este trimis utilizatorului prin e-mail sau accesat prin aplicații media; **Aspecte critice** • Afectează aplicațiile media și jocurile care utilizează **DirectX**; • Exploatarea poate fi automatizată prin streaming media compromis. **Măsuri de remediere** • Aplicarea patch-urilor cumulative oferite de Microsoft; • Utilizarea de soluții de securitate pentru a detecta fișiere media malițioase; • Restricționarea descărcării și redării fișierelor media din surse nesigure.