CVE-2025-21297

Scor/Severitate	8.1 (CRITIC)
CWE-ID	**CWE-416** – Use After Free
Sisteme afectate	❖ Windows Server 2019 – cu rol RD Gateway activ ❖ Windows Server 2022 – afectat implicit ❖ Alte versiuni Windows cu Remote Desktop Gateway expus public
Componente afectate	• *Windows Remote Desktop Gateway* (RD Gateway)
Descriere	CVE-2025-21297 este o vulnerabilitate critică în componenta *Remote Desktop Gateway* a *Windows* Server. Exploatarea cu succes a vulnerabilității permite unui atacator neautentificat să execute cod arbitrar în contextul procesului serviciului, cu posibilitatea de compromitere completă a serverului.
Metode de exploatare	1. Atacatorul trimite cereri multiple manipulate în paralel către *RD Gateway*. 2. Se declanșează o condiție de cursă în modul în care serviciul procesează sesiunile *RDP*. 3. Este posibilă scrierea în memorie neprotejată, urmată de injectarea de shellcode. 4. Shellcode-ul este executat cu privilegii *SYSTEM* în contextul procesului ***tsgateway.exe***.
Etapele de exploatare	**1.** Reconnaissance (Recunoaștere) • Atacatorul identifică o instanță de *RD Gateway* expusă public (de obicei pe portul TCP 443). • Se verifică prezența componentei tsgateway.exe și se detectează comportamentul serviciului prin analiză pasivă sau scanări. **2.** Inițializare conexiuni multiple • Atacatorul deschide mai multe conexiuni *HTTPS* către *RD Gateway*, cu payload-uri manipulate. • Se folosesc scripturi sau instrumente care controlează timpii de transmitere pentru a declanșa o execuție concurentă (concurrency). **3.** Declanșarea condiției de cursă (race condition) • Două sau mai multe fire de execuție din tsgateway.exe accesează simultan resurse comune: ✓ Structuri de memorie nesincronizate ✓ Buffere temporare sau sesiuni *TLS*/*RDP* **4.** Coruperea memoriei (memory corruption) • În urma competiției dintre thread-uri, unul dintre ele: ✓ finalizează validarea fără verificări complete; ✓ permite acces la structuri neinițializate; ✓ expune o zonă de memorie unde atacatorul poate scrie date arbitrare (payload). **5.** Injectare de shellcode • Atacatorul injectează un payload (de tip shellcode sau ROP chain) într-o locație controlată din memoria procesului tsgateway.exe. • Acest payload este proiectat să ofere execuție de cod arbitrar în contextul procesului. **6.** Execuția codului arbitrar (Remote Code Execution) • Codul injecat este executat de procesul afectat, oferind atacatorului: ✓ execuție la nivel *SYSTEM*;

<table>
<tr><td></td><td colspan="2">✓ deschidere reverse shell către serverul C2;
✓ inițiere backdoor sau livrare ransomware.
7. Persistență și mișcare laterală
• După exploatare, atacatorul poate:
✓ instala instrumente persistente (ex. Cobalt Strike, Sliver);
✓ accesa alte sisteme prin WMI, PsExec, SMB lateral movement;
✓ extrage date, token-uri, sau chei Active Directory.</td></tr>
<tr><td rowspan="7">IOC</td><td>Tip</td><td>Exemplu</td></tr>
<tr><td>Hash PoC</td><td>7d8c2b193ab312d1ef89aa6c5a1e4e6e1c3b0aef789c1...</td></tr>
<tr><td>Proces vizat</td><td>tsgateway.exe</td></tr>
<tr><td>Adresă IP rău famat</td><td>185.100.87.50</td></tr>
<tr><td>Domeniu C2</td><td>rdgw-access[.]com</td></tr>
<tr><td>Porturi implicate</td><td>Default: TCP 443 (HTTPS), UDP 3391 (UDP pentru RDP over SSL)</td></tr>
<tr><td>Tehnologie subiacente</td><td>HTTP.sys, RDP protocol stack, WinHTTP, RPC, TLS Layer</td></tr>
<tr><td>Metode de detectare</td><td colspan="2">• Comportament proces RDG - Activitate anormală în tsgateway.exe.
• Rețea - Cereri RDP simultane și neobișnuite de la aceeași sursă IP.
• Memorie - Analiza heap/dump pentru payload shellcode activ.
• EDR/XDR - Detectare de injecție în proces și pattern-uri Cobalt Strike.</td></tr>
<tr><td>Metode de remediere</td><td colspan="2">• Aplicați patch-ul oficial oferit de Microsoft (dacă disponibil)
• Restricționați accesul la RD Gateway doar prin VPN sau IP-uri whitelisted
• Activați și monitorizați IDS/IPS pentru semnale de trafic RDP anormal
• Utilizați EDR care detectează proces injection și condiții de cursă
• Auditați configurările RD Gateway și dezactivați expunerea externă dacă nu este necesară</td></tr>
<tr><td>Vulnerabilități exploatabile ulterior</td><td colspan="2">CVE-2023-23397 – Outlook Privilege Escalation
CVE-2021-34527 – PrintNightmare
CVE-2022-30190 – Follina MSDT RCE</td></tr>
<tr><td>Referință</td><td colspan="2">https://securityonline.info/cve-2025-21297-race-condition-in-windows-remote-desktop-gateway-enables-rce-poc-demonstrates-exploitability/
https://nvd.nist.gov/vuln/detail/cve-2025-21297</td></tr>
</table>