Raport consolidat eveniment cibernetic

CVE-2024-49039

CVE-2024-49039 este o vulnerabilitate critică în componenta **Windows Task Scheduler**, care permite unui atacator local să escaladeze privilegiile prin exploatarea necorespunzătoare a apelurilor RPC (Remote Procedure Call). Problema apare din cauza validării incomplete a permisiunilor la nivelul serviciului Task Scheduler.

Informații suplimentare

TIP	**CVE**
Platforme afectate	Windows 10, Windows Server 2016/ 2019/ 2022
Vectori de atac	❖ Precondiții exploatare: ✓ Acces local la sistem. ✓ Privilegii scăzute (cont de utilizator local sau acces minim). ✓ Nu necesită interacțiunea utilizatorului. ❖ Impact: ✓ Escaladare de privilegii locale la nivel de ***System***. ✓ Acces la funcții și date restricționate. ✓ Posibilitatea de a instala programe malițioase sau a modifica setări critice de securitate.

Mecanism de exploatare	❖ Acces local la sistem: ✓ Atacatorul compromite un cont de utilizator cu acces limitat, fie prin tehnici de phishing, exploatarea altor vulnerabilități sau prin malware. ❖ Manipularea Task Scheduler: ✓ Task Scheduler utilizează RPC pentru interacțiunea cu componentele sistemului. ✓ O cerere RPC special creată permite atacatorului să ocolească măsurile de securitate. ✓ Exemplu: Un atacator poate injecta cod malițios pentru a rula comenzi arbitrare cu privilegii de sistem. ❖ Escaladarea Privilegilor: ✓ Exploatarea reușită permite atacatorului să acceseze și să modifice resurse critice ale sistemului: • Instalarea backdoor-urilor. • Modificarea politicilor de securitate. • Acces complet la fișiere sensibile și resurse administrative.
Exemplu de cod	Exemplu simplificat pentru a ilustra abordarea: ***„import os*** ***import ctypes*** ***# Simularea unei cereri RPC malițioase*** ***def exploit_task_scheduler():*** ***# Conexiune către serviciul Task Scheduler*** ***task_scheduler_handle = ctypes.windll.advapi32.OpenServiceA(*** ***"localhost",*** ***"Schedule",*** ***0xF01FF # Permisiuni complete*** ***)*** ***if not task_scheduler_handle:*** ***print("Eșec la conectarea la Task Scheduler")*** ***return*** ***# Executarea codului malițios*** ***ctypes.windll.advapi32.ControlService(*** ***task_scheduler_handle,*** ***1, # Comanda de execuție*** ***ctypes.byref(ctypes.c_int(0))***

```
    )
    print("Exploatare reușită!")
exploit_task_scheduler()”
```

Exemplu te cod de exploatare:

```
„#include <windows.h>
#include <rpc.h>
void ExploitTaskScheduler() {
    RPC_STATUS status;
    RPC_BINDING_HANDLE handle;
    WCHAR *stringBinding;
    // Crearea unei legături RPC
    status = RpcStringBindingComposeW(
        NULL,
        (RPC_WSTR)L"ncacn_np",
        (RPC_WSTR)L"\\\\localhost",
        (RPC_WSTR)L"\\pipe\\atsvc",
        NULL,
        &stringBinding
    );
    if (status != RPC_S_OK) {
        printf("Eroare la crearea legăturii RPC\n");
        return;
    }
    // Legarea la server
    status = RpcBindingFromStringBindingW(stringBinding, &handle);
    if (status != RPC_S_OK) {
        printf("Eroare la legarea RPC\n");
        return;
    }
    // Aici se trimite payload-ul malițios
    // (Pentru siguranță, această secțiune este redată abstractă)
```

	printf("Trimitem payload malițios...\n"); ***RpcBindingFree(&handle);*** ***RpcStringFreeW(&stringBinding);*** ***}*** ***int main() {*** ***ExploitTaskScheduler();*** ***return 0;*** ***}”***
Impactul Exploatării	❖ Confidențialitate: ✓ Acces la date sensibile stocate pe sistem. ✓ Posibilitatea de a intercepta comunicațiile locale. ❖ Integritate: ✓ Modificarea fișierelor și setărilor critice. ✓ Coruperea aplicațiilor și a datelor sistemului. ❖ Disponibilitate: ✓ Dezactivarea serviciilor esențiale. ✓ Blocarea completă a sistemului prin ransomware.
Măsuri de remediere	❖ Actualizări sofware: ✓ **Patch-uri Critice:** Microsoft a lansat actualizări pentru a remedia această vulnerabilitate. Verificați și aplicați ultimele update-uri: • Pagina Microsoft Security Response Center (MSRC) • Update-ul de securitate din **Noiembrie 2024** pentru Windows ❖ Restricționarea Accesului: ✓ Limitați permisiunile pentru conturile de utilizator locale. ✓ Configurați **Applocker** pentru a bloca executarea fișierelor neautorizate. ❖ Hardening al Sistemului: ✓ Implementați protecții AppLocker sau SRP (Software Restriction Policies) pentru a controla ce aplicații pot fi executate de utilizatorii neprivilegiați.

- ✓ Activați funcții de securitate avansate, precum Credential Guard și Exploit Protection.

❖ Monitorizarea și Detectarea:
- ✓ Utilizați soluții EDR (Endpoint Detection and Response) pentru a monitoriza activitatea Task Scheduler.
- ✓ Activați jurnalizarea avansată în Windows (Audit Policy) pentru a identifica apeluri RPC suspecte: ***„auditpol /set /subcategory:"Service Creation" /success:enable /failure:enable”***

❖ Măsuri de Prevenire:
- ✓**Izolare Aplicații:** Utilizați tehnici de sandboxing pentru a limita impactul aplicațiilor compromise.
- ✓**Restricționarea RPC:** Implementați reguli în firewall pentru a restricționa apelurile RPC nesigure.

Resurse externe

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-49039

https://nvd.nist.gov/vuln/detail/CVE-2024-49039

https://www.cve.org/CVERecord?id=CVE-2024-49039