Esercizio S5_L4_BONUS W11_TOP_CVEs

Vulnerabilità CVE in Windows 11 (2023–2025)

In ambito cybersecurity, è fondamentale conoscere e comprendere le vulnerabilità note relative ai principali sistemi operativi. Questo report presenta un'analisi delle vulnerabilità CVE più rilevanti emerse negli ultimi anni su Windows 11, evidenziando per ciascuna il meccanismo d'azione, l'impatto potenziale e le contromisure consigliate.

CVE critici in Windows 11 (ultimi 2–3 anni)

CVE-2023-38146 – ThemeBleed (RCE)

È stata identificata una vulnerabilità di esecuzione di codice remoto (RCE) nel motore di gestione dei temi di Windows. Il problema risiede nella gestione di file .theme e .deskthemepack, i quali non vengono validati correttamente durante il parsing.

- **Gravità:** CVSS 8.8 – Critico
- **Impatto:** esecuzione arbitraria di codice al livello utente, potenzialmente senza intervento attivo.
- **Sistemi affetti:** tutte le versioni di Windows 11 antecedenti alla patch.
- **Patch:** disponibile tramite aggiornamento cumulativo Microsoft (Patch Tuesday ottobre 2023).

CVE-2024-30085 – Escalation locale dei privilegi

Durante il contest TyphoonPWN 2024, è stata scoperta una vulnerabilità che consente a un utente locale di ottenere privilegi SYSTEM attraverso una falla nel gestore delle policy di sicurezza.

- **Gravità stimata:** ~CVSS 9.0
- **Impatto:** elevazione dei privilegi locali, utile per persistence e privilege escalation post-exploit.
- **Versione impattata**: Windows 11 versione 23H2
- **Patch:** corretta da Microsoft poco dopo la divulgazione pubblica.

CVE-2024-38063 – Overflow via IPv6 (tcpip.sys)

È stato rilevato un overflow heap nel driver di rete tcpip.sys, attivabile tramite pacchetti IPv6 appositamente formattati. L'exploit consente potenzialmente l'esecuzione di codice in modalità kernel da remoto.

- **Gravità:** CVSS 9.8 – Critico
- **Impatto:** esecuzione remota di codice con privilegi kernel (RCE)
- **Sistemi affetti**: Windows 11 e Windows 10
- **Patch:** rilasciata con l'aggiornamento di agosto 2024.

CVE-2024-43451 / CVE-2024-49039 – Attacchi NTLM e Task Scheduler

Due vulnerabilità scoperte in parallelo permettono:

- La compromissione di credenziali NTLM (CVE-43451);
- L'elevazione dei privilegi tramite il Task Scheduler (CVE-49039).
-

Entrambe sono state osservate in campagne attive di attacco ("zero-day in the wild").

- **Gravità:** 6.5 (43451) e 8.8 (49039)
- **Impatto**: furto credenziali e privilege escalation
- **Patch:** disponibile da novembre 2024

CVE-2025-47981 – RCE via SPNEGO (Kerberos)

Un heap overflow nella componente SPNEGO di Kerberos può essere sfruttato da remoto e senza autenticazione per eseguire codice arbitrario.

- **Gravità:** Critico
- **Impatto**: esecuzione remota senza autenticazione
- **Versioni colpite**: Windows 11 (22H2, 23H2, 24H2)
- **Patch:** contenuta negli aggiornamenti di luglio 2025

CVE-2025-48822 – RCE Hyper-V DDA

Nel contesto di Hyper-V, la funzionalità Discrete Device Assignment (DDA) espone una vulnerabilità che consente a una macchina guest di eseguire codice sulla macchina host.

- **Gravità**: CVSS 8.6
- **Impatto**: esecuzione di codice da guest su host
- **Versioni vulnerabili**: Windows 11 (tutte fino alla 24H2), Windows Server
- **Mitigazione**: applicare aggiornamento cumulativo di luglio 2025

CVE-2025-48799 – EoP nel servizio Windows Update

Il servizio Windows Update soffre di un problema legato alla gestione di link simbolici ("link following"), che consente a un attaccante locale di sovrascrivere file di sistema.

- **Gravità:** CVSS 7.8
- **Impatto:** escalazione privilegi
- **Patch:** inclusa nella patch Microsoft di luglio 2025

Approfondimento Tecnico

CVE-2024-38063 – *Remote Code Execution via IPv6*

Questa vulnerabilità risiede nel modulo tcpip.sys, componente fondamentale per la gestione dello stack di rete. Il driver, nel processo di parsing dei pacchetti IPv6, non implementa adeguate verifiche dei limiti in alcuni campi del pacchetto, causando un overflow controllabile in heap.

Sfruttamento:

Un attaccante può inviare pacchetti IPv6 malformati a un host con IPv6 attivo. Il parsing dei pacchetti provoca scritture out-of-bounds, che possono essere manipolate per iniettare codice eseguibile in modalità kernel.

PoC disponibili:

Diversi proof-of-concept sono stati resi noti su blog tecnici come MalwareTech e Picus Security.

Mitigazioni consigliate:

- Disabilitare temporaneamente IPv6, se non strettamente necessario.
- Applicare l'aggiornamento di agosto 2024.
- Utilizzare un firewall per filtrare il traffico IPv6 in ingresso.

CVE-2023-38146 – *ThemeBleed (Windows Themes RCE)*

Il motore di rendering dei temi Windows non verifica correttamente alcuni puntatori e buffer all'interno di file .theme. Questo può permettere un attacco RCE sfruttando la semplice apertura (o preview) di un file tema dannoso.

Vettore di attacco:

L'attaccante predispone un file .theme contenente codice dannoso. L'utente può attivare l'exploit semplicemente visualizzando l'anteprima del tema, anche in modalità sandbox, se le policy non sono restrittive.

Proof-of-Concept:

È stato pubblicato un PoC su GitHub che dimostra come, tramite un file .deskthemepack, sia possibile avviare una shell di sistema.

Mitigazioni:

- Disabilitare il supporto ai temi personalizzati, se non necessario.
- Applicare l'aggiornamento Microsoft rilasciato a ottobre 2023.
- Usare AppLocker per bloccare esecuzione di file .theme da percorsi non attendibili.

Raccomandazioni generali per la sicurezza

Per ridurre il rischio derivante da queste e altre vulnerabilità:

1. Applicare regolarmente gli aggiornamenti di sicurezza, in particolare quelli rilasciati nei Patch Tuesday mensili.
2. Utilizzare il principio del privilegio minimo, limitando i diritti degli utenti locali.
3. Monitorare le interfacce di rete, specialmente il traffico IPv6 non richiesto.
4. Utilizzare firewall, EDR e antivirus aggiornati per individuare tentativi di exploit in tempo reale.
5. Tenere sotto controllo le fonti ufficiali, come il Microsoft Security Update Guide, il National Vulnerability Database (NVD), e le notifiche CISA.