

# Relazione sulle Vulnerabilità di Sicurezza di Windows 10 (CVE)

Le vulnerabilità di sicurezza nei sistemi operativi come Windows 10 rappresentano una minaccia significativa per la protezione dei dati e la sicurezza delle infrastrutture IT. Con l'evolversi delle tecniche di attacco e l'intensificarsi delle minacce provenienti da attori malintenzionati, è fondamentale comprendere i rischi associati a queste vulnerabilità, le loro implicazioni e come mitigare tali pericoli. Di seguito, vengono analizzate alcune delle principali vulnerabilità relative a Windows 10, con un focus sulle soluzioni adottabili per proteggere i sistemi.

## 1. CVE-2024-21431: Vulnerabilità nel Sistema di Aggiornamento di Windows

Gravità: Alta (CVSS 7.8)

Descrizione: Questa vulnerabilità consente a un attaccante locale di elevare i privilegi sul sistema sfruttando debolezze nel processo di aggiornamento. L'esecuzione di codice con privilegi elevati potrebbe compromettere l'intero sistema, consentendo a un aggressore di acquisire il controllo del dispositivo.

Implicazioni: Se non corretta, la vulnerabilità potrebbe essere sfruttata da attaccanti locali per ottenere diritti di amministratore, compromettendo l'integrità del sistema.

Soluzione: L'unico modo per prevenire il rischio è applicare tempestivamente gli aggiornamenti di sicurezza rilasciati da Microsoft. È fondamentale che le organizzazioni mantengano aggiornati i propri sistemi, specialmente quelli esposti a Internet, per evitare exploit.

## 2. CVE-2024-21430: Bypass delle Funzionalità HVCI

Gravità: Media (CVSS 5.7)

Descrizione: La vulnerabilità relativa a Hypervisor-Protected Code Integrity (HVCI) consente di bypassare alcune delle protezioni avanzate progettate per evitare l'esecuzione di codice dannoso a livello di sistema. L'abilitazione di HVCI è una misura di sicurezza cruciale per proteggere il sistema

da exploit che mirano a corrompere il codice di basso livello.

Implicazioni: Un attaccante potrebbe aggirare le protezioni, compromettere il sistema e eseguire codice non autorizzato, aumentando il rischio di attacchi avanzati e persistenti.

Soluzione: È essenziale configurare correttamente HVCI e aggiornare periodicamente Windows 10 per implementare le correzioni. L'adozione di altre misure di sicurezza come Device Guard contribuisce a rafforzare il sistema contro attacchi di questo tipo.

### 3. CVE-2022-21882: Escalation dei Privilegi Tramite Win32k.sys

Gravità: Alta (CVSS 7.0)

Descrizione: Questa vulnerabilità nel driver Win32k.sys permette a un attaccante di elevare i propri privilegi locali, ottenendo accesso a livello di amministratore. Questo tipo di vulnerabilità è particolarmente preoccupante poiché gli attacchi che sfruttano errori nei driver di sistema sono spesso difficili da rilevare e possono essere utilizzati per eseguire codice dannoso senza il consenso dell'utente.

Implicazioni: L'attaccante potrebbe eseguire codice arbitrario con privilegi elevati, accedere a informazioni riservate e compromettere la stabilità del sistema. Questa vulnerabilità è stata già sfruttata da gruppi di attacco avanzati (APT).

Soluzione: Microsoft ha rilasciato una patch di sicurezza che corregge la vulnerabilità. Gli utenti devono applicare immediatamente questi aggiornamenti per ridurre i rischi legati all'escalation dei privilegi.

### 4. CVE-2024-30051: Vulnerabilità nel Driver USB Hub

Gravità: Alta (CVSS 7.8)

Descrizione: Un attaccante potrebbe sfruttare questa vulnerabilità per eseguire codice arbitrario attraverso dispositivi USB malintenzionati. Il driver USB Hub di Windows 10 è vulnerabile a exploit che potrebbero essere sfruttati per ottenere l'accesso remoto al sistema.

Implicazioni: L'attaccante potrebbe compromettere la macchina target semplicemente introducendo

un dispositivo USB manipolato. Questo scenario è particolarmente rischioso in ambienti aziendali dove le porte USB sono ampiamente utilizzate.

Soluzione: Oltre ad applicare le patch di sicurezza, è importante limitare l'accesso ai dispositivi USB non autorizzati e monitorare costantemente le periferiche connesse. In contesti aziendali, si consiglia di implementare politiche di controllo delle periferiche USB.

## 5. CVE-2015-1769: Vulnerabilità nel Windows Mount Manager

Gravità: Alta (CVSS 7.8)

Descrizione: Questa vulnerabilità nel Windows Mount Manager consente a un attaccante di eseguire codice dannoso quando un dispositivo di archiviazione esterno viene connesso al sistema. Il rischio è che l'attaccante possa guadagnare l'accesso al sistema e acquisire privilegi di amministratore.

Implicazioni: Il rischio è elevato, poiché gli attacchi USB sono una delle tecniche più comuni per distribuire malware. Gli attaccanti potrebbero infettare il sistema senza che l'utente se ne accorga.

Soluzione: Per proteggere i sistemi da exploit USB, è fondamentale applicare le patch di sicurezza e limitare l'accesso a dispositivi non fidati. Inoltre, il monitoraggio costante dei dispositivi collegati può prevenire attacchi di questo tipo.

## Conclusioni e Raccomandazioni

Le vulnerabilità esaminate evidenziano l'importanza di un approccio proattivo alla sicurezza dei sistemi Windows 10. Per mitigare i rischi associati a queste falle, è cruciale:

1. Applicare gli aggiornamenti di sicurezza non appena disponibili.
2. Abilitare le funzionalità di sicurezza avanzate, come HVCI e Device Guard, per proteggere il sistema da exploit.
3. Controllare rigorosamente l'accesso ai dispositivi esterni, specialmente USB, e monitorare le periferiche connesse.

4. Utilizzare il principio del minor privilegio per ridurre il rischio di escalations di privilegi da parte degli attaccanti.

Implementando queste misure, le organizzazioni e gli utenti possono ridurre significativamente il rischio di attacchi informatici e garantire la sicurezza dei loro sistemi Windows 10.