Vulnerabilità Windows 11

1. CVE-2024-38124: Windows Netlogon Elevation of Privilege Vulnerability

Descrizione: La vulnerabilità riguarda il protocollo Netlogon, che gestisce l'autenticazione per i sistemi Windows. Un attaccante potrebbe sfruttare un errore di validazione nei pacchetti Netlogon per eseguire codice arbitrario con privilegi elevati. Questo permette di bypassare la protezione di autenticazione, dando all'attaccante accesso a risorse e dati sensibili.

Impatto: Consente l'escalation dei privilegi da parte di un attaccante con accesso a un account utente con privilegi limitati, fino a ottenere i privilegi di amministratore, permettendo l'accesso a dati sensibili, l'esecuzione di codice dannoso o la modifica di configurazioni critiche.

CVSS: 9.0 (Critica)

Soluzione: Microsoft ha rilasciato una patch di sicurezza che corregge questa vulnerabilità, quindi è essenziale applicare l'aggiornamento tramite Windows Update. La vulnerabilità può essere mitigata monitorando i log di sistema e assicurandosi che le configurazioni di rete siano corrette per limitare l'esposizione di Netlogon. (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38124)

2. CVE-2024-21412: Windows Shortcuts Security Bypass Vulnerability

Descrizione: Questa vulnerabilità si verifica nel trattamento dei file di collegamento (.lnk) in Windows. I file di collegamento possono essere usati da attaccanti per eseguire codice malevolo senza che l'utente sia avvertito dai meccanismi di protezione di Windows. Il sistema di gestione dei collegamenti non valida correttamente i target, permettendo ai file dannosi di bypassare i controlli di sicurezza come SmartScreen.

Impatto: Gli aggressori possono utilizzare i file di collegamento per aggirare le protezioni, portando all'esecuzione di malware o ransomware. Un utente potrebbe essere indotto a fare clic su un file di collegamento, che potrebbe innescare l'esecuzione del codice dannoso.

CVSS: 8.8 (Alta)

Soluzione: La soluzione consiste nell'installare l'aggiornamento di sicurezza fornito da Microsoft che corregge il trattamento dei collegamenti. È anche consigliato evitare di aprire file .lnk sospetti e non scaricare collegamenti da fonti non verificate.
(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21412)

3. CVE-2024-21351: Windows SmartScreen Security Bypass Vulnerability

Descrizione: SmartScreen, il sistema di difesa integrato in Windows per identificare e bloccare file e siti web pericolosi, presenta una vulnerabilità che consente a file dannosi di bypassare il controllo. In pratica, file malformati possono essere ingannare SmartScreen, evitando la sua rilevazione e il suo blocco.

Impatto: Consente l'esecuzione di malware che sarebbe normalmente bloccato dal sistema di protezione. Gli attaccanti possono sfruttare questa vulnerabilità per distribuire software dannoso tramite email di phishing, siti web compromessi o download di file pericolosi.

CVSS: 8.0 (Alta)

Soluzione: L'aggiornamento di sicurezza risolve questa vulnerabilità modificando il comportamento di SmartScreen per rilevare più efficacemente i file dannosi. È fondamentale aggiornare Windows 11 per chiudere questa falla di sicurezza. Inoltre, si consiglia di utilizzare sempre il filtro SmartScreen per file e siti web e di non aprire allegati sospetti.
(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21351)

4. CVE-2024-43451: NTLMv2 Hash Spoofing Vulnerability

Descrizione: NTLMv2 è un protocollo di autenticazione utilizzato da Windows. Un attaccante potrebbe sfruttare una vulnerabilità nel processo di validazione dell'hash NTLMv2 per impersonare un altro utente sulla rete, aggirando i controlli di autenticazione e ottenendo accesso non autorizzato. Questo attacco sfrutta la possibilità di falsificare gli hash NTLMv2 utilizzati per autenticarsi su risorse di rete.

Impatto: L'attaccante potrebbe accedere a risorse di rete senza essere autenticato correttamente, eseguire comandi con privilegi elevati e compromettere la sicurezza della rete aziendale o domestica.

CVSS: 7.8 (Alta)

Soluzione: Microsoft consiglia di sostituire l'autenticazione NTLM con Kerberos dove possibile, poiché quest'ultimo è più sicuro e meno vulnerabile. In caso di utilizzo di NTLM, è importante monitorare i log di sicurezza per rilevare tentativi di spoofing. Aggiornare il sistema e configurare correttamente le politiche di rete è cruciale per mitigare questo rischio.
(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-43451)

5. CVE-2024-21348: Windows Kernel Elevation of Privilege Vulnerability

Descrizione: Il kernel di Windows è il cuore del sistema operativo, gestendo risorse di basso livello come processi e memoria. Una vulnerabilità in Windows 11 consente a un attaccante

di eseguire codice non autorizzato con privilegi elevati, aggirando la protezione del kernel e ottenendo il pieno controllo del sistema.

Impatto: Un attaccante con accesso limitato potrebbe eseguire codice dannoso con privilegi di sistema, compromettendo completamente la macchina. Questo attacco potrebbe portare all'installazione di rootkit, spyware, o altre forme di malware avanzato.

CVSS: 9.0 (Critica)

Soluzione: Microsoft ha rilasciato una patch di sicurezza che corregge il bug nel kernel. È fondamentale aggiornare il sistema per proteggere i dispositivi vulnerabili. Inoltre, adottare il principio del minimo privilegio e garantire che solo gli utenti essenziali abbiano privilegi di amministratore può ridurre i danni di un potenziale exploit.
(https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-21348)