Ipostesi di remediation - vulnerabilità MS08-067

Vulnerabilità MS08-067

La vulnerabilità MS08-067 è una delle vulnerabilità più famose associata a Microsoft Windows, in particolare a causa del suo utilizzo nel worm Conficker che ha infettato milioni di computer nel 2008 e 2009.

Ecco una breve descrizione:

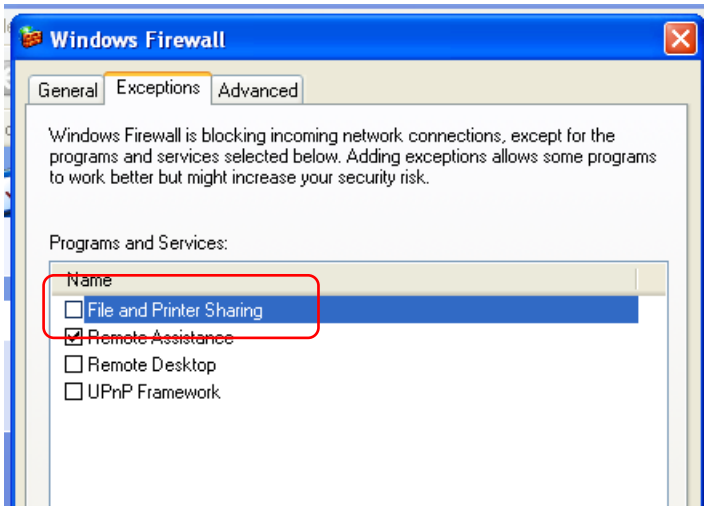
- **Nome completo**: MS08-067 - Vulnerabilità nella gestione del server RPC potrebbe consentire l'esecuzione di codice remoto (958644)
- **Componente vulnerabile**: Il componente vulnerabile in Windows è la gestione del Server RPC (Remote Procedure Call) nel netapi32.dll.
- **Impatto**: Se sfruttata con successo, questa vulnerabilità potrebbe permettere a un aggressore di eseguire codice arbitrario in un sistema target, dando all'aggressore il pieno controllo del sistema.
- **Causa**: La vulnerabilità è dovuta a una mancata corretta gestione delle richieste RPC. Un attaccante potrebbe inviare una richiesta RPC artigianale che potrebbe portare all'esecuzione di codice.
- **Sistemi interessati**: Diverse versioni di Microsoft Windows, tra cui Windows 2000, Windows XP e Windows Server 2003, sono vulnerabili.
- **Popolarità**: Questa vulnerabilità è stata ampiamente sfruttata da malware e worm, il più noto dei quali è Conficker.
- **Mitigazione**: Microsoft ha rilasciato una patch per questa vulnerabilità nel 2008. Pertanto, l'aggiornamento dei sistemi con l'ultima patch di sicurezza previene l'exploit.

Ipotesi di remediation

Disabilitare la condivisione di file e stampanti

Disabilitando la condivisione di file e stampanti dal Firewall di Windows la vulnerabilità non può essere sfruttata. Tuttavia, questa è un'operazione che ha grande impatto sull'operatività aziendale, rendendo impossibile lavorare su file e stampanti condivise dalla macchina in questione.

Questa remediation potrebbe essere usata temporaneamente prima di trovare una soluzione con minore impatto sull'operatività.



Soluzioni al controllo di webcam e tastiera

Se si è certi che processi remoti non autorizzati stiano acquisendo dati tramite tastiera e/o webcam, possiamo risolvere temporaneamente oscurando la webcam se è integrata o scollegandola in caso contrario. Nella maggior parte dei casi questo ha impatto minimo poiché la webcam non è uno strumento essenziale per la maggior parte delle attività.

Nel caso della tastiera, potremmo utilizzare la tastiera su schermo. in questo moso il mouse sarebbe l'unica periferica utilizzata, impedendo al keylogger di catturare i dati delle nostre digitazioni. Tuttavia, questa è una soluzione molto scomoda che rende molto più lenta la digitazione con grande impatto sull'operatività. Potrebbe essere usata solo temporaneamente in attesa di implementare una remediation migliore.

Applicazione della patch

La soluzione più diretta e ovvia per questa specifica vulnerabilità è applicare l'aggiornamento di sicurezza fornito da Microsoft. La patch MS08-067 è disponibile da Microsoft ed è stata rilasciata poco dopo la scoperta della vulnerabilità.