REPORT SCANSIONE WINDOWS7 CON NESSUS

Scopo:

Il presente rapporto si enfoca sull'analisi delle vulnerabilità rilevate mediante la scansione del sistema operativo Windows 7 tramite Nessus, un'applicazione dedicata alla sicurezza informatica. L'obbiettivo è individuare le vulnerabilità critiche e pianificare interventi correttivi per mitigare i rischi associati.

Contesto:

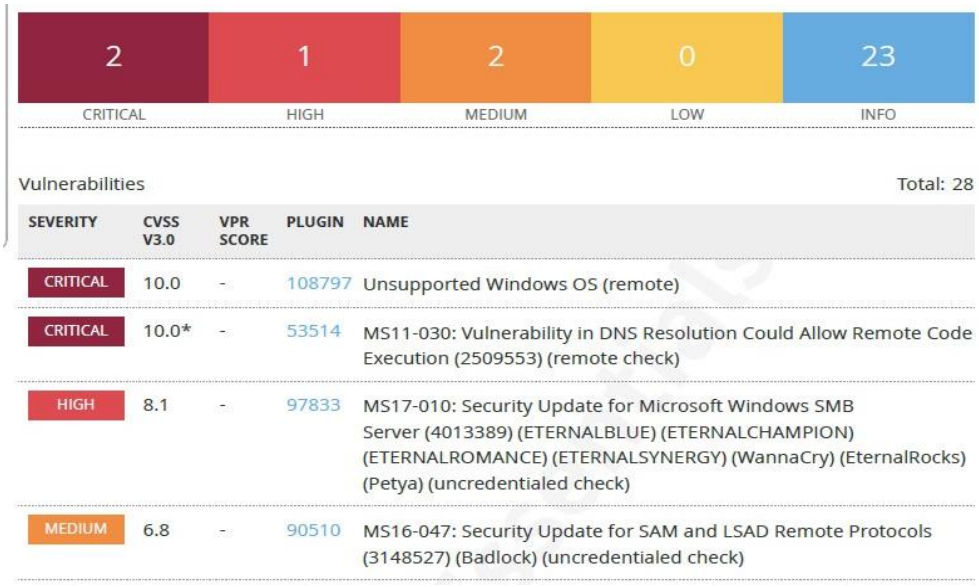
Il sistema esaminato tramite la scansione è un'istanza di Windows 7, ampiamente diffuso in contesti aziendali e personali. Identificare e risolvere le vulnerabilità critiche su questo sistema riveste importanza cruciale per garantire la sicurezza e la protezione dei dati sensibili.

Metodologia:

Abbiamo impiegato Nessus, un tool di scansione ampiamente riconosciuto nel campo della sicurezza informatica, per eseguire una scansione completa del sistema operativo Windows 7. L'applicazione ha analizzato il sistema alla ricerca di vulnerabilità note e possibili punti di attacco.

Risultati:

Durante la fase iniziale della scansione, sono state individuate diverse vulnerabilità. Successivamente, procederemo con l'analisi e la risoluzione di quattro di esse in particolare.

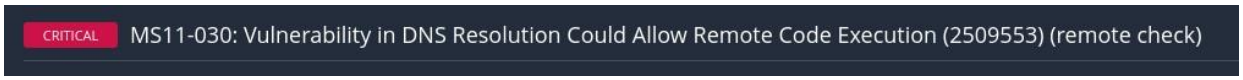


2	1	2	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 28

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	-	53514	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
MEDIUM	6.8	-	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)

1



Relazione sulla Vulnerabilità Critica MS11-030 su Windows 7

Analisi della Vulnerabilità:

La vulnerabilità critica individuata con il codice MS11-030 coinvolge il risolutore DNS di Windows, presentando il rischio di consentire l'esecuzione remota di codice nel contesto dell'account NetworkService. Tale vulnerabilità sfrutta il processo di elaborazione delle query Link-local Multicast Name Resolution (LLMNR) da parte del client DNS di Windows.

Il risolutore DNS di Windows, presente nelle versioni Vista, 2008, 7 e 2008 R2, può essere sfruttato da un attaccante remoto per l'esecuzione di codice arbitrario. Contrariamente, su Windows XP e 2003, che non supportano LLMNR, l'attacco riuscito richiede accesso locale e la capacità di eseguire un'applicazione speciale.

Proposte di Intervento:

1. Applicazione delle Patch di Sicurezza: Microsoft ha rilasciato un insieme di patch volte a correggere questa vulnerabilità su Windows XP, 2003, Vista, 2008, 7 e 2008 R2. Si raccomanda l'installazione immediata delle patch pertinenti per il sistema operativo Windows 7 al fine di ridurre il rischio di sfruttamento della vulnerabilità.

2. Configurazione del Firewall: Nel frattempo, è possibile adottare regole firewall per limitare l'accesso ai servizi vulnerabili, compresi i servizi DNS, allo scopo di diminuire la superficie di attacco e mitigare il rischio di exploit, fino a quando le patch di sicurezza non vengono applicate.

Conclusione:

La vulnerabilità MS11-030 costituisce una minaccia rilevante per la sicurezza dei sistemi Windows 7, consentendo agli attaccanti di eseguire codice arbitrario da remoto. È imperativo applicare le patch di

sicurezza fornite da Microsoft e implementare ulteriori misure di protezione, come la configurazione del firewall, al fine di mitigare in modo efficace il rischio di compromissione del sistema.

2

Report sulla Vulnerabilità Critica "Unsupported Windows OS" su Windows 7

Analisi della Vulnerabilità:

La vulnerabilità critica "Unsupported Windows OS" indica che la versione di Microsoft Windows in uso non dispone di un service pack supportato o non è più supportata da Microsoft. Questo significa che il sistema operativo è suscettibile a contenere vulnerabilità di sicurezza, poiché non riceve più aggiornamenti di sicurezza e correzioni di bug da parte di Microsoft.

Nel caso specifico, il sistema operativo Microsoft Windows 7 Home è identificato come non supportato.

Azioni di Rimedio Proposte:

1. **Aggiornamento a un Service Pack Supportato o a un Sistema Operativo Supportato:** La soluzione primaria per risolvere questa vulnerabilità è aggiornare il sistema operativo a una versione supportata da Microsoft o applicare l'ultimo service pack disponibile per la versione attualmente in uso. Questo garantirà che il sistema riceva regolarmente gli aggiornamenti di sicurezza e le correzioni di vulnerabilità necessarie per proteggere il sistema dagli attacchi informatici.

2. **Valutazione delle Opzioni di Aggiornamento:** Nel caso in cui l'aggiornamento a un service pack supportato non sia possibile o praticabile, è consigliabile valutare l'opzione di aggiornare a una versione di sistema operativo supportata, come Windows 10. Questo assicurerà che il sistema sia protetto da futuri rischi di sicurezza e che riceva il supporto continuo da parte di Microsoft.

Conclusione:

La presenza di un sistema operativo non supportato su un host rappresenta una seria minaccia per la sicurezza, poiché espone il sistema a vulnerabilità di sicurezza note e non riceve più aggiornamenti per proteggere da tali rischi. È fondamentale prendere provvedimenti immediati per aggiornare il sistema operativo a una versione supportata o applicare il service pack più recente disponibile per mitigare il rischio di compromissione del sistema.

3

Relazione sulla Vulnerabilità MS17-010 su Windows

Analisi della Vulnerabilità:

La vulnerabilità MS17-010, comunemente nota come EternalBlue, rappresenta una delle vulnerabilità più gravi e sfruttate sui sistemi operativi Windows. Questa falla coinvolge il protocollo Server Message Block 1.0 (SMBv1), impiegato per la condivisione di file e stampanti nelle reti Windows.

La vulnerabilità consente a un attaccante remoto non autenticato di eseguire codice arbitrario sul sistema bersaglio, sfruttando difetti nell'elaborazione di richieste specifiche di SMBv1. Ciò significa che l'attaccante può sfruttare la vulnerabilità per condurre attacchi di esecuzione remota del codice (RCE) e ottenere il controllo completo del sistema.

Oltre alla possibilità di eseguire codice arbitrario, la vulnerabilità MS17-010 può essere sfruttata per rivelare informazioni sensibili sul sistema, costituendo così un serio rischio per la sicurezza e la privacy dei dati.

Azioni di Rimedio Proposte:

1. Applicazione delle Patch di Sicurezza: Microsoft ha rilasciato un insieme di patch volte a correggere questa vulnerabilità su una vasta gamma di sistemi operativi Windows, inclusi Windows Vista, 7, 8.1, 10 e le relative versioni server. È imperativo applicare immediatamente tali patch per proteggere i sistemi vulnerabili dall'exploit di EternalBlue.

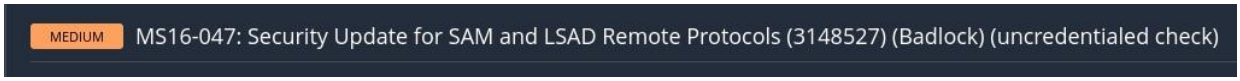
2. Disabilitazione di SMBv1: Per i sistemi operativi Windows non supportati, quali Windows XP e 2003, per i quali non sono disponibili patch di sicurezza, Microsoft consiglia di disabilitare SMBv1. Questo può essere effettuato seguendo le istruzioni fornite da Microsoft nel Knowledge Base (KB2696547). Inoltre, si consiglia di bloccare direttamente il traffico SMB bloccando le porte TCP 445 e le porte UDP 137/138/139 su tutti i dispositivi di rete.

3. Monitoraggio del Traffico di Rete: Implementare una rigorosa politica di monitoraggio del traffico di rete per identificare e bloccare eventuali tentativi di sfruttamento della vulnerabilità MS17-010. Utilizzare soluzioni avanzate di sicurezza informatica per rilevare e mitigare il traffico sospetto sulla rete.

Conclusione:

La vulnerabilità MS17-010 costituisce una minaccia estremamente grave per la sicurezza dei sistemi Windows, potenzialmente causando gravi conseguenze come la compromissione completa del sistema e la perdita di dati sensibili. È essenziale applicare le patch di sicurezza fornite da Microsoft e adottare misure aggiuntive per mitigare il rischio di sfruttamento della vulnerabilità MS17-010, preservando così l'integrità e la sicurezza del sistema.

4



Relazione sulla Vulnerabilità MS16-047 su Windows

Analisi della Vulnerabilità:

La vulnerabilità MS16-047, conosciuta anche come Badlock, rappresenta un problema di elevazione dei privilegi che coinvolge i protocolli di Remote Procedure Call (RPC) utilizzati per la gestione degli account di sicurezza (SAM) e delle autorità di sicurezza locali (LSAD) su sistemi operativi Windows.

Questa falla consente a un attaccante in grado di intercettare le comunicazioni tra un client e un server che ospita un database SAM di forzare il livello di autenticazione a scendere, permettendo all'attaccante di impersonare un utente autenticato e accedere al database SAM.

Azioni di Rimedio Proposte:

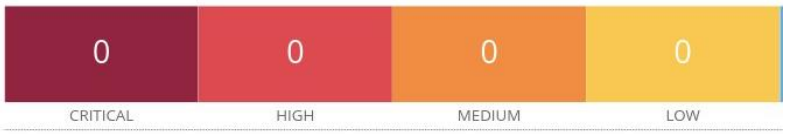
1. Applicazione delle Patch di Sicurezza: Microsoft ha rilasciato un insieme di patch mirate a risolvere questa vulnerabilità su una vasta gamma di sistemi operativi Windows, inclusi Windows Vista, 7, 8.1, 10 e le relative versioni server. È imperativo applicare immediatamente tali patch per proteggere i sistemi vulnerabili dall'exploit di Badlock.

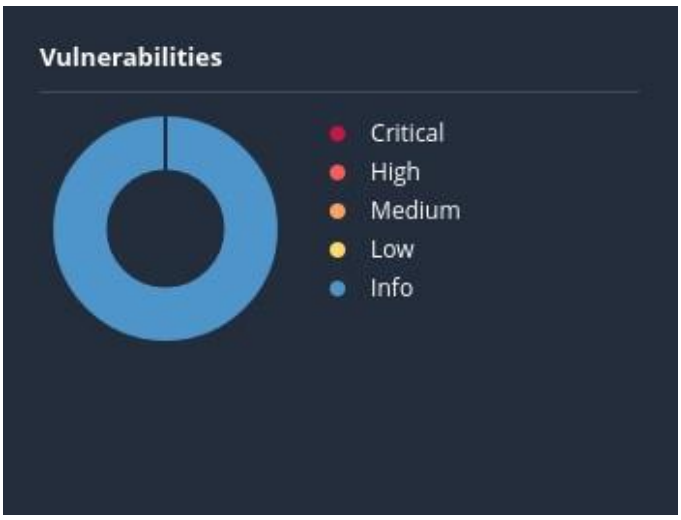
2. Implementazione di Misure di Sicurezza Aggiuntive: Per ridurre il rischio di sfruttamento della vulnerabilità MS16-047, si consiglia di adottare misure di sicurezza supplementari, come l'utilizzo di firme digitali per autenticare le comunicazioni RPC, il monitoraggio del traffico di rete per individuare attività sospette e l'applicazione di controlli di accesso rigorosi per limitare l'accesso ai database SAM solo agli utenti autorizzati.

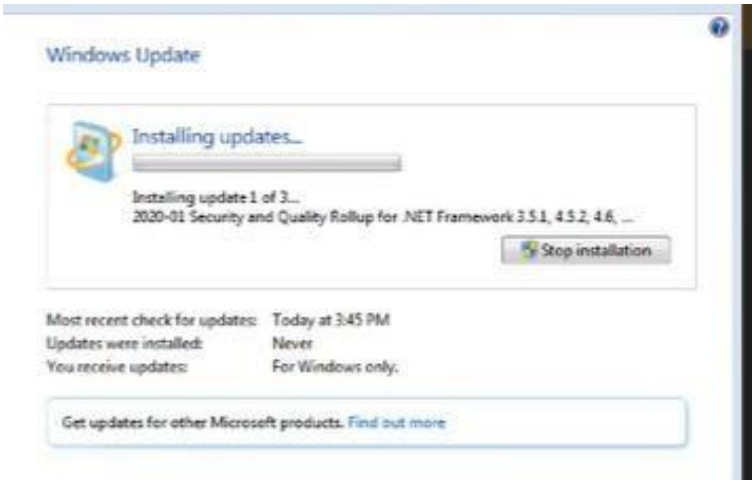
Conclusione:

La vulnerabilità MS16-047 costituisce una minaccia significativa per la sicurezza dei sistemi Windows, potenzialmente portando a gravi conseguenze come la compromissione del database SAM e la violazione della sicurezza dei dati. È essenziale applicare le patch di sicurezza fornite da Microsoft e adottare misure aggiuntive per mitigare il rischio di sfruttamento della vulnerabilità MS16-047, preservando così l'integrità e la sicurezza del sistema.

RISOLUZIONE DELLE VULNERABILITA' DOPO NUOVA SCANSIONE







Relazione sulla Vulnerabilità MS16-047 su Windows

Analisi della Vulnerabilità:

La vulnerabilità MS16-047, nota anche come Badlock, rappresenta una problematica di elevazione dei privilegi che coinvolge i protocolli di Remote Procedure Call (RPC) utilizzati per la gestione degli account di sicurezza (SAM) e delle autorità di sicurezza locali (LSAD) sui sistemi operativi Windows.

Questo difetto consente a un attaccante, capace di intercettare le comunicazioni tra un client e un server ospitante un database SAM, di costringere il livello di autenticazione a scendere. Ciò permette all'attaccante di impersonare un utente autenticato e ottenere accesso al database SAM.

Azioni di Rimedio Proposte:

1. Applicazione delle Patch di Sicurezza: Microsoft ha rilasciato un insieme di patch finalizzate a risolvere questa vulnerabilità su una vasta gamma di sistemi operativi Windows, compresi Windows Vista, 7, 8.1, 10 e le relative versioni server. È essenziale applicare immediatamente tali patch per proteggere i sistemi vulnerabili dall'exploit di Badlock.

2. Implementazione di Misure di Sicurezza Aggiuntive: Al fine di ridurre il rischio di sfruttamento della vulnerabilità MS16-047, si raccomanda l'adozione di misure di sicurezza supplementari, come l'utilizzo di firme digitali per autenticare le comunicazioni RPC, il monitoraggio del traffico di rete per rilevare attività sospette e l'attuazione di controlli di accesso rigorosi per limitare l'accesso ai database SAM solo agli utenti autorizzati.

Conclusione:

La vulnerabilità MS16-047 rappresenta una minaccia significativa per la sicurezza dei sistemi Windows, potenzialmente portando a gravi conseguenze come la compromissione del database SAM e la violazione della sicurezza dei dati. È fondamentale applicare le patch di sicurezza fornite da Microsoft e adottare misure aggiuntive per mitigare il rischio di sfruttamento della vulnerabilità MS16-047, preservando così l'integrità e la sicurezza del sistema.