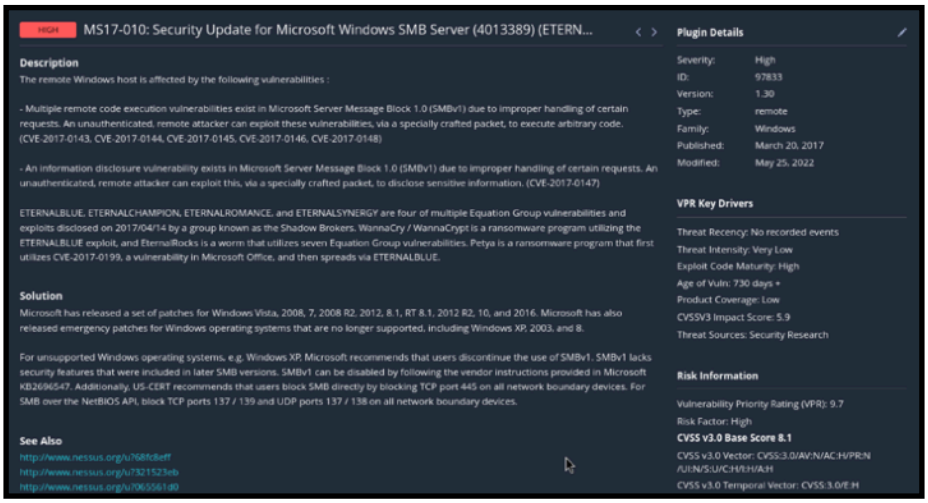
M3_W12D4

Remediation Action.

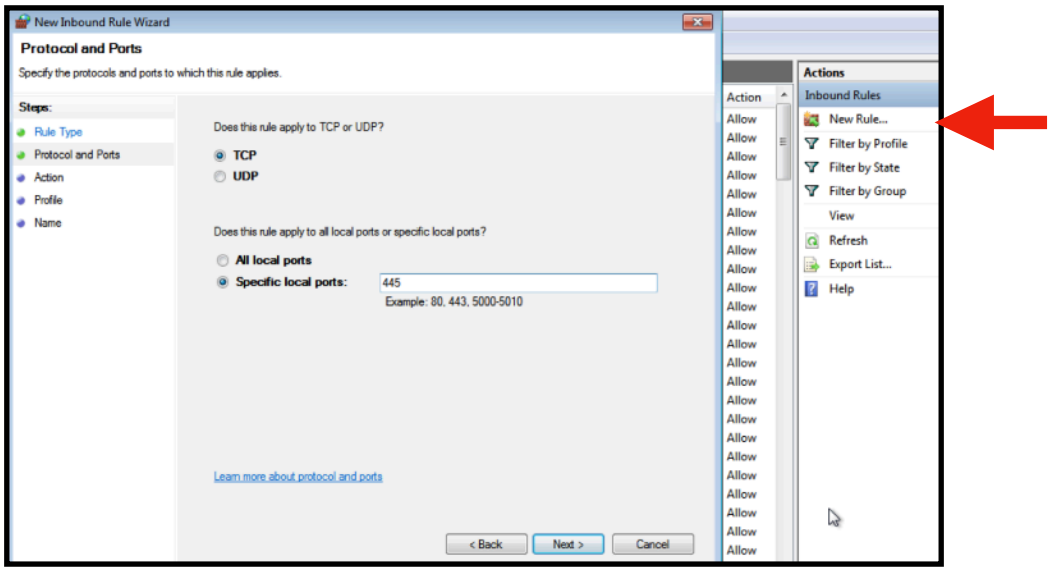
1. MS17-0-10 identificata da Nessus come una vulnerabilità high-level.



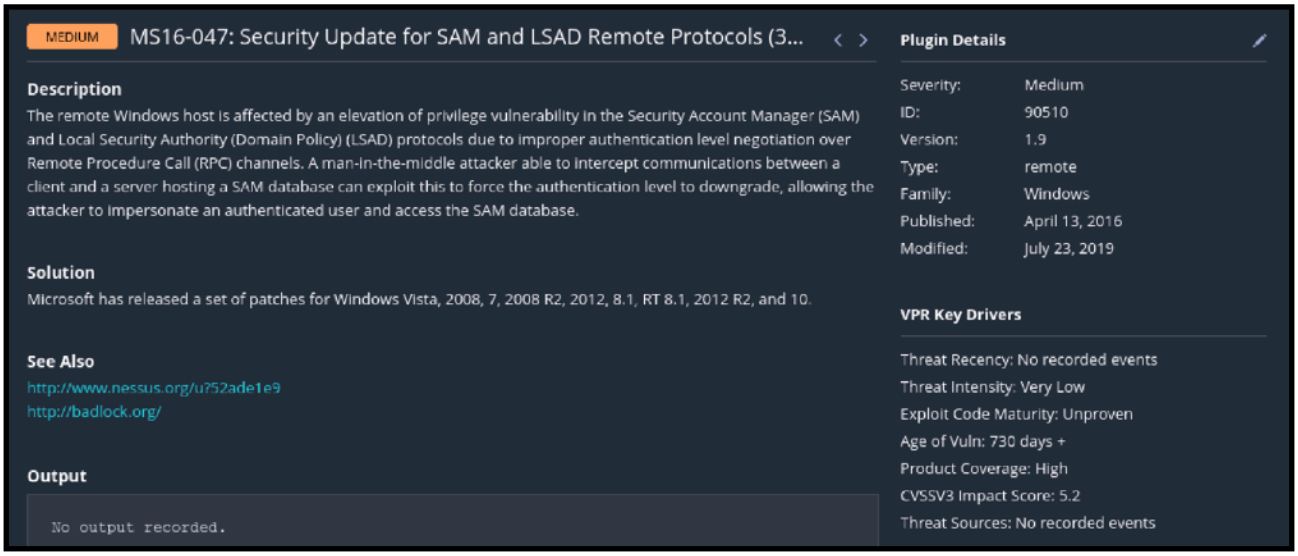
Esistono più vulnerabilità di esecuzione di codice remoto in Microsoft Server Message Block 1.0 (SMBv1)
Esiste una vulnerabilità di divulgazione delle informazioni in Microsoft Server Message Block 1.0 (SMBv1) a causa della gestione impropria di alcune richieste. Un attaccante remoto non autenticato può sfruttare questo problema, tramite un pacchetto appositamente creato, per divulgare informazioni sensibili.

Soluzione: Si proseguirà con la chiusura della porta TCP/445.

Proseguiamo con la configurazione di una policy sul Firewall di Windows. Selezionando Inbound Rules > New Rules dalle impostazioni avanzate del firewall di Windows chiuderemo la porta TCP/445 (come in figura) bloccando il traffico in entrata su di essa. Dopo aver confermato la nuova regola il firewall è pronto a filtrare il traffico diretto sulla porta in questione.

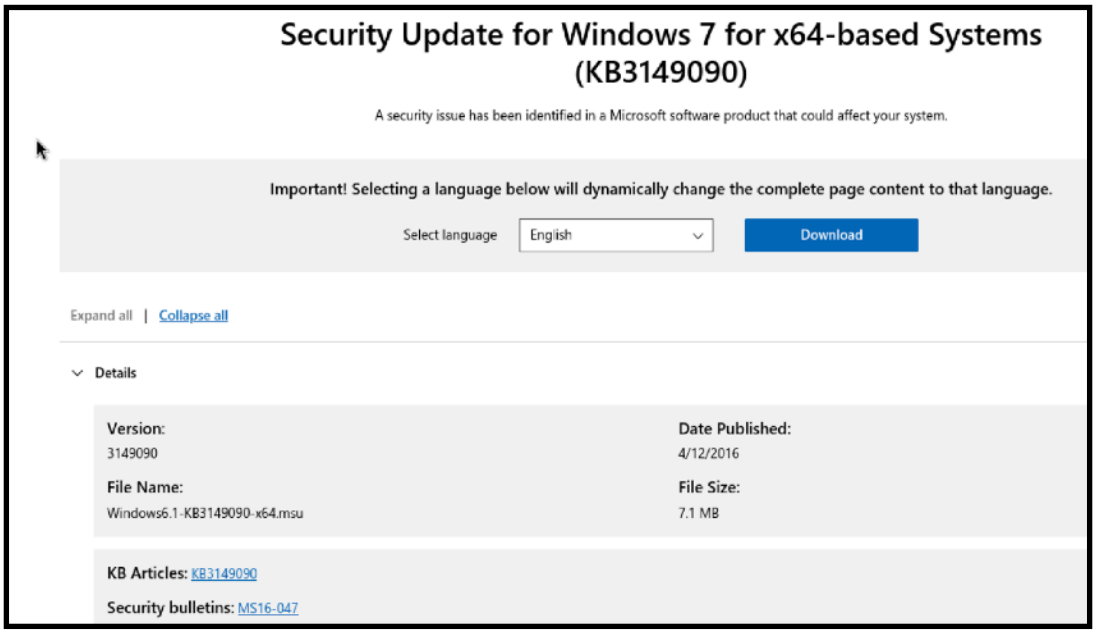


2. MS16-047 identificata da Nessus come una vulnerabilità medium level.



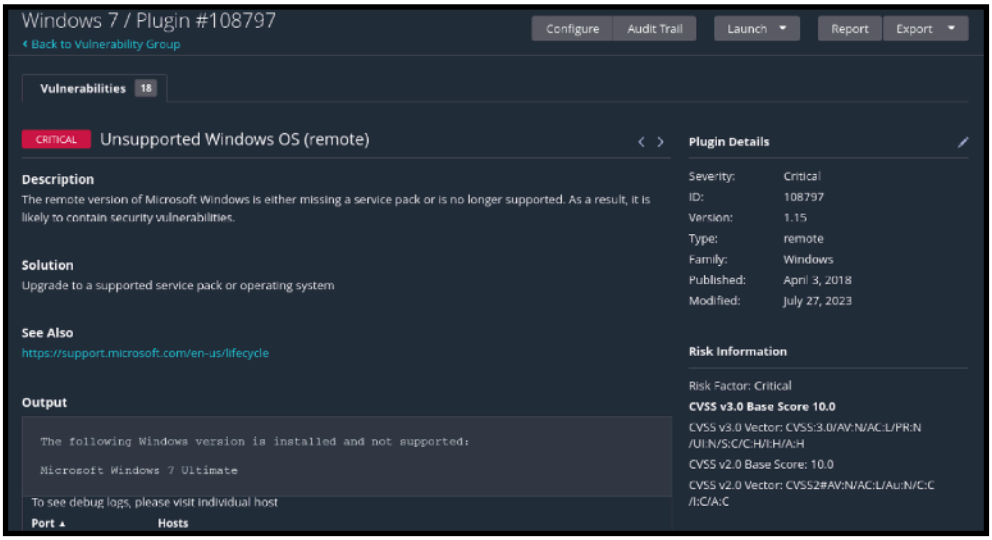
Secondo Nessus l'host Windows remoto è affetto da una vulnerabilità di elevazione dei privilegi nei protocolli Security Account Manager (SAM) e Local Security Authority (Domain Policy) (LSAD) dovuta a una negoziazione impropria del livello di autenticazione sui canali Remote Procedure Call (RPC). Un utente malintenzionato in grado di intercettare le comunicazioni tra un client e un server che ospita un database SAM può sfruttare questa vulnerabilità per forzare il declassamento del livello di autenticazione, consentendo all'aggressore di impersonare un utente autenticato e accedere al database SAM.

Soluzione: Proseguire con il download delle patches su Windows.



Ultimato il download il rischio che un attaccante possa sfruttare questa vulnerabilità è quasi nullo.

3. Unsupported Windows OS identificata come una vulnerabilità critica.



Nessus indica che la versione remota di Microsoft Windows è priva di un service pack o non è più supportata. Di conseguenza, è altamente probabile che contenga vulnerabilità di sicurezza.

Soluzione: Aggiornare service pack o al sistema operativo supportato.

(Poiché Windows 7 risulterà utile per lo studio di ulteriori vulnerabilità non aggiorneremo il sistema operativo consapevoli che la vulnerabilità in esame sarebbe stata fixata)