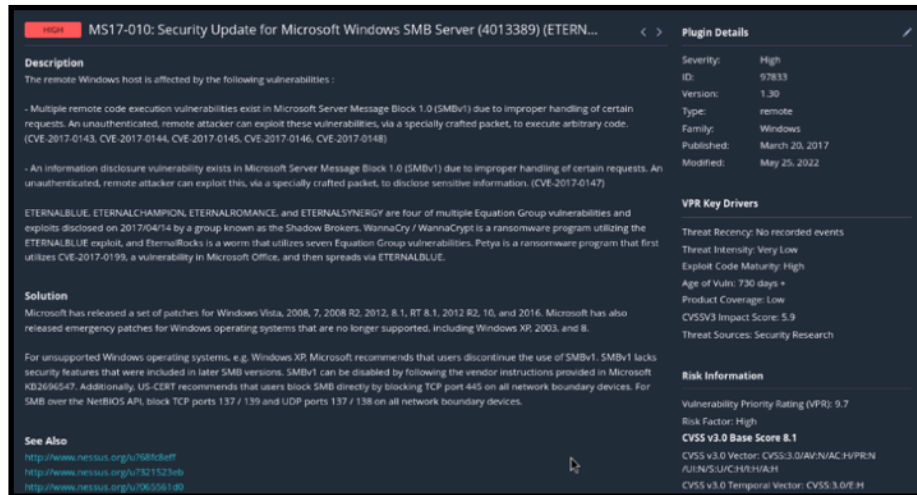


M3_W12D4

Remediation Action.

1. **MS17-010** identificata da Nessus come una vulnerabilità high-level.

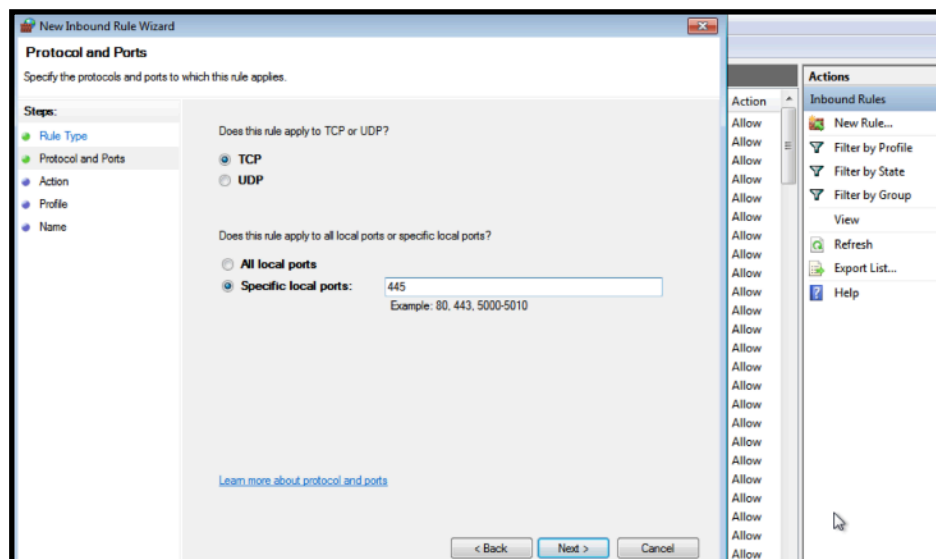


Esistono più vulnerabilità di esecuzione di codice remoto in Microsoft Server Message Block 1.0 (SMBv1)

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.

MEDIUM MS16-047: Security Update for SAM and LSAD Remote Protocols (3... < >

Description

The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database.

Solution

Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10.

See Also

<http://www.nessus.org/u752ade1e9>
<http://badlock.org/>

Output

No output recorded.

Plugin Details

Severity: Medium
ID: 90510
Version: 1.9
Type: remote
Family: Windows
Published: April 13, 2016
Modified: July 23, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: High
CVSSV3 Impact Score: 5.2
Threat Sources: No recorded events

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.

Security Update for Windows 7 for x64-based Systems (KB3149090)

A security issue has been identified in a Microsoft software product that could affect your system.

Important! Selecting a language below will dynamically change the complete page content to that language.

Select language

Expand all | [Collapse all](#)

Details

Version:	3149090	Date Published:	4/12/2016
File Name:	Windows6.1-KB3149090-x64.msu	File Size:	7.1 MB

KB Articles: [KB3149090](#)
Security bulletins: [MS16-047](#)

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

3. **Unsupported Windows OS** identificata come una vulnerabilità critica.

The screenshot shows the Nessus interface for a vulnerability report. At the top, it says 'Windows 7 / Plugin #108797' with buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this is a 'Vulnerabilities' section with a count of 18. The main section is titled 'Unsupported Windows OS (remote)' and is marked as 'CRITICAL'. It includes a 'Description' stating that the remote version of Microsoft Windows is either missing a service pack or is no longer supported, likely containing security vulnerabilities. A 'Solution' suggests upgrading to a supported service pack or operating system. A 'See Also' link points to <https://support.microsoft.com/en-us/lifecycle>. The 'Output' section shows a message: 'The following Windows version is installed and not supported: Microsoft Windows 7 Ultimate. To see debug logs, please visit individual host'. On the right, 'Plugin Details' lists: Severity: Critical, ID: 108797, Version: 1.15, Type: remote, Family: Windows, Published: April 3, 2018, Modified: July 27, 2023. Below this, 'Risk Information' shows a Risk Factor of Critical and a CVSS v3.0 Base Score of 10.0. The CVSS v3.0 Vector is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H. The CVSS v2.0 Base Score is 10.0. The CVSS v2.0 Vector is CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C.

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)