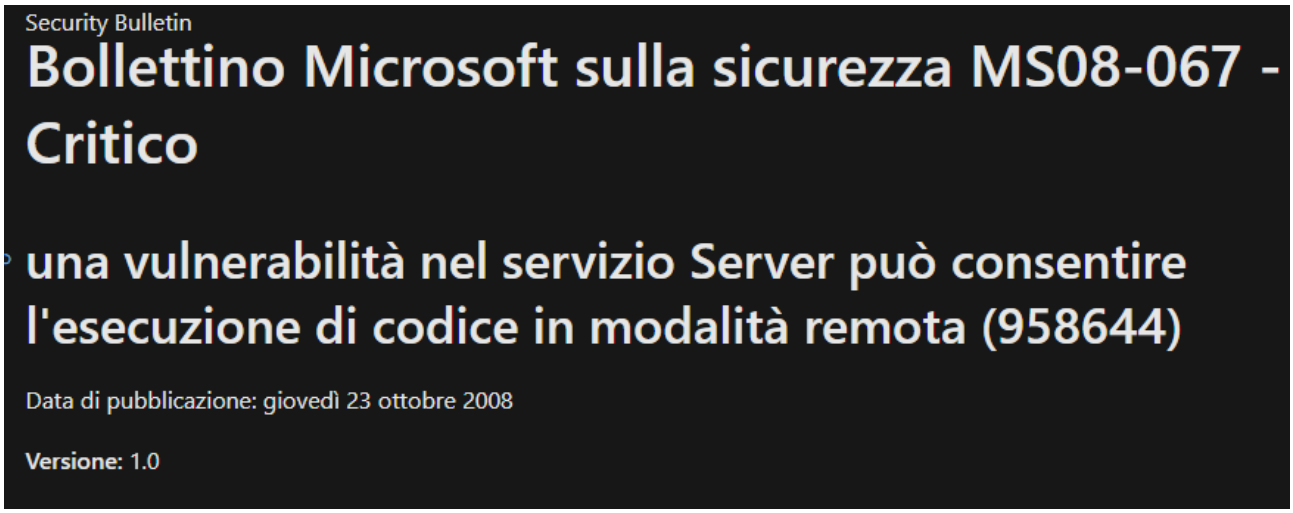
Introduzione esercizio



Come possiamo vedere dal Microsoft Bulletin la vulnerabilità in questione permette l'esecuzione di codice arbitrario sulla macchina con i seguenti sistemi operativi.

Sistema operativo	Livello massimo di impatto sulla protezione	Livello di gravità aggregato	Bollettini so aggiorname
Microsoft Windows 2000 Service Pack 4	Esecuzione di codice in modalità remota	Critico	MS06-040
Windows XP Service Pack 2	Esecuzione di codice in modalità remota	Critico	MS06-040
Windows XP Service Pack 3	Esecuzione di codice in modalità remota	Critico	Nessuno
Windows XP Professional x64 Edition	Esecuzione di codice in modalità remota	Critico	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Esecuzione di codice in modalità remota	Critico	Nessuno
Windows Server 2003 Service Pack 1	Esecuzione di codice in modalità remota	Critico	MS06-040
Windows Server 2003 Service Pack 2	Esecuzione di codice in modalità remota	Critico	Nessuno
Windows Server 2003 x64 Edition	Esecuzione di codice in modalità remota	Critico	MS06-040
Windows Server 2003 x64 Edition Service Pack 2	Esecuzione di codice in modalità remota	Critico	Nessuno
Windows Server 2003 con SP1 per sistemi basati su Itanium	Esecuzione di codice in modalità remota	Critico	MS06-040

Sistema operativo	Livello massimo di impatto sulla protezione	Livello di gravità aggregato	Bollettini so aggiorname
Windows Server 2003 con SP2 per sistemi basati su Itanium	Esecuzione di codice in modalità remota	Critico	Nessuno
Windows Vista e Windows Vista Service Pack 1	Esecuzione di codice in modalità remota	Importante	Nessuno
Windows Vista x64 Edition e Windows Vista x64 Edition Service Pack 1	Esecuzione di codice in modalità remota	Importante	Nessuno
Windows Server 2008 per sistemi a 32 bit*	Esecuzione di codice in modalità remota	Importante	Nessuno
Windows Server 2008 per sistemi x64*	Esecuzione di codice in modalità remota	Importante	Nessuno
Windows Server 2008 per sistemi basati su Itanium	Esecuzione di codice in modalità remota	Importante	Nessuno

Windows XP rientra le macchine interessate e, pertanto, possiamo utilizzare l'exploit Eternal Blue per avere accesso alla macchina e controllarla a distanza, eseguendo privilege excalation, lateral movement, file deletion (nel video), snapshot della macchina, rimozione dell'antivirus, abbassamento del firewall e così via.

Eventuali remediation actions:

1- Aggiornamento del sistema operativo ad una versione avanzata. Sebbene Microsoft "Il 13 maggio 2017, un giorno dopo l'attacco, Microsoft ha inusualmente fornito, tramite un download dal Microsoft Update Catalog, un aggiornamento di sicurezza volto a eliminare la sopraccitata vulnerabilità anche da versioni di Microsoft Windows non più supportate, ossia Windows XP, Windows 8, e Windows Server 2003", l'aggiornamento del SO è la base per una vita sicura online.
2- Innalzamento del Firewall. Come sappiamo, la chiusura o il filtraggio delle porte non permette una scansione accurata da parte dei tool come nmap, nessus ecc.., pertanto renderemo la vita più difficile ad un eventuale attaccante.
3- Possiamo eventualmente risolvere anche solo la vulnerabilità SMB v1.0, facendo l'upgrade ad una versione più recente a partire dalla 2.0 in poi
4- Per quanto riguarda l'uso di periferiche hardware, ho scoperto che una tastiera wireless può essere intercettata a molti metri di distanza! Non è necessario ai fini dell'esercizio ma è comunque qualcosa da tenere in conto durante l'acquisto dell'hardware. Per quanto riguarda la webcam, possiamo acquistare a poco prezzo una clip che la copra (https://www.amazon.it/ACERFULL-Copri-Microfibra-Camera-Cover-Accessori-Sottile-Copri-Portatile-iPhone-Tablet-Smartphones-Noteboook-Webcam/dp/B0BWS9TXN9/ref=sr_1_5?__mk_it_IT=%C3%85M%C3%85%C5%BD%C3%95%C3%91&crid=2Z8XCV6V7352B&keywords=webcam+cover&qid=1687420362&sprefix=webcam+cove%2Caps%2C132&sr=8-5) oppure mantenerla staccata dallo slot USB, accendendola solo quando necessario.