BASIC NETWORK SCAN - WINDOWS XP

Report generated by Nessus™ Mon, 19 Jun 2023 04:08:14 EDT

TABLE OF CONTENTS

Vulnerabilità per Host

Vulnerabilità per Host

192.168.90.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	1	0	0	1

Scan Information

Start time: Mon Jun 19 04:04:46 2023
End time: Mon Jun 19 04:08:14 2023

Host Information

Netbios Name: WINDOWSXPSP3
IP: 192.168.90.101
MAC Address: 08:00:27:D1:5D:39
OS: Microsoft Windows XP Service Pack 2, Microsoft Windows XP Service Pack 3, Windows XP for Embedded Systems

Vulnerabilities

34477 - MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check)

Synopsis

L'host Windows remoto è interessato da una vulnerabilità legata all'esecuzione di codice in modalità remota.

Description

L'host Windows remoto è interessato da una vulnerabilità legata all'esecuzione di codice in modalità remota nel servizio "Server" dovuto
alla gestione impropria delle richieste RPC. Un utente malintenzionato remoto non autenticato può sfruttarlo tramite un file special
richiesta RPC predisposta, per eseguire codice arbitrario con "Sistema"
privilegi.
ECLIPSEDWING è una delle molteplici vulnerabilità ed exploit di Equation Group divulgate il 14/04/2017 da un gruppo noto come Shadow Brokers.

See Also

https://www.nessus.org/u?adf86aac

Solution

Microsoft ha rilasciato una serie di patch per Windows 2000, XP, 2003, Vista e 2008.

Fattore di rischio

Critico

Punteggio base CVSS v3.0

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio temporale CVSS v3.0

9.4 (CVSS:3.0/E:H/RL:O/RC:C)

Punteggio VPR

9.4

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Punteggio temporale CVSS v2.0

8.7 (CVSS2#E:H/RL:OF/RC:C)

STIG Gravità

IO

Riferimenti

OFFERTA	31874
CVE	CVE-2008-4250
MSKB	958644
XRIF	MSFT:MS08-067
XRIF	CERT:827267
XRIF	IAVA:2008-A-0081-S
XRIF	EDB-ID:6824
XRIF	EDB-ID:7104
XRIF	EDB-ID:7132
XRIF	CWE:94

Sfruttabile con

CANVAS (vero) Core Impact (vero) Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 23/10/2008, Modificato: 05/08/2020

Uscita del plug-in

tcp/445/cifs

35362 - MS09-001: Vulnerabilità di Microsoft Windows SMB Esecuzione di codice in modalità remota (958687) (controllo senza credenziali)

Sinossi

È possibile arrestare in modo anomalo l'host remoto a causa di un difetto in SMB.

Descrizione

L'host remoto è interessato da una vulnerabilità di danneggiamento della memoria in SMB che potrebbe consentire a un utente malintenzionato di eseguire codice arbitrario o eseguire una negazione del servizio contro l'host remoto.

Guarda anche

http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx

Soluzione

Microsoft ha rilasciato una serie di patch per Windows 2000, XP, 2003, Vista e 2008.

Fattore di rischio

Critico

Punteggio VPR

7.4

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Punteggio temporale CVSS v2.0

7.8 (CVSS2#E:POC/RL:OF/RC:C)

Riferimenti

OFFERTA	31179
OFFERTA	33121
OFFERTA	33122
CVE	CVE-2008-4834
CVE	CVE-2008-4835
CVE	CVE-2008-4114
MSKB	958687
XRIF	MSFT:MS09-001
XRIF	CWE: 399

Sfruttabile con

Core Impact (vero) Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 13/01/2009, Modificato: 08/06/2023

Uscita del plug-in

tcp/445/cifs

108797 - Sistema operativo Windows non supportato (remoto)

Sinossi

Il sistema operativo remoto o il service pack non sono più supportati.

Descrizione

La versione remota di Microsoft Windows non dispone di un service pack o non è più supportata. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Guarda anche

https://support.microsoft.com/en-us/lifecycle

Soluzione

Eseguire l'upgrade a un service pack o sistema operativo supportato

Fattore di rischio

Critico

Punteggio base CVSS v3.0

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Punteggio base CVSS v2.0

10.0 (CVSS2#AV:N/CA:S/Au:N/DO:DO/MI:DO/LA:DO)

Riferimenti

XRIF IAV:0001-A-0501

Informazioni sul plug-in

Pubblicato: 03/04/2018, Modificato: 05/07/2022

Uscita del plug-in

TCP/0

La seguente versione di Windows è installata e non è supportata:

Microsoft Windows XP Service Pack 2

Microsoft Windows XP Service Pack 3

Windows XP per sistemi integrati

97833 - MS17-010: Aggiornamento della protezione per Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (controllo senza credenziali)

Sinossi

L'host Windows remoto è interessato da più vulnerabilità.

Descrizione

L'host Windows remoto è interessato dalle seguenti vulnerabilità:

- Esistono più vulnerabilità legate all'esecuzione di codice in modalità remota in Microsoft Server Message Block 1.0 (SMBv1) a causa della gestione impropria di determinate richieste. Un utente malintenzionato remoto non autenticato può sfruttare queste vulnerabilità, tramite un pacchetto appositamente predisposto, per eseguire codice arbitrario. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- Esiste una vulnerabilità alla divulgazione di informazioni in Microsoft Server Message Block 1.0 (SMBv1) a causa della gestione impropria di determinate richieste. Un utente malintenzionato remoto non autenticato può sfruttarlo, tramite un pacchetto appositamente predisposto, per divulgare informazioni riservate. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE ed ETERNALSYNERGY sono quattro delle molteplici vulnerabilità ed exploit di Equation Group divulgate il 14/04/2017 da un gruppo noto come Shadow Brokers. WannaCry / WannaCrypt è un programma ransomware che utilizza l'exploit ETERNALBLUE ed EternalRocks è un worm che sfrutta sette vulnerabilità di Equation Group. Petya è un programma ransomware che prima utilizza CVE-2017-0199, una vulnerabilità in Microsoft Office, e poi si diffonde tramite ETERNALBLUE.

Guarda anche

http://www.nessus.org/u?68fc8eff http://www.nessus.org/u?321523eb http://
www.nessus.org/u?065561d0 http://www.nessus.org/u ?d9f569cf https://
blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ http://
www.nessus.org/u?b9d9ebf9

http://www.nessus.org/u?8dcab5e4 http://
www.nessus.org/u?234f8ef8 http://
www.nessus.org/u?4c7e0cf3 https://github.com/
stamparm/EternalRocks / http://
www.nessus.org/u?59db5b5b

Soluzione

Microsoft ha rilasciato una serie di patch per Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 e 2016. Microsoft ha inoltre rilasciato patch di emergenza per i sistemi operativi Windows che non sono più supportati, tra cui Windows XP, 2003 e 8.

Per i sistemi operativi Windows non supportati, ad esempio Windows XP, Microsoft consiglia agli utenti di interrompere l'uso di SMBv1. SMBv1 non dispone delle funzionalità di sicurezza incluse nelle versioni successive di SMB.

SMBv1 può essere disabilitato seguendo le istruzioni del fornitore fornite in Microsoft KB2696547. Inoltre, US-CERT consiglia agli utenti di bloccare SMB direttamente bloccando la porta TCP 445 su tutti i dispositivi di confine della rete. Per SMB sull'API NetBIOS, bloccare le porte TCP 137/139 e le porte UDP 137/138 su tutti i dispositivi di confine della rete.

Fattore di rischio

Alto

Punteggio base CVSS v3.0

8.1 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio temporale CVSS v3.0

7.7 (CVSS:3.0/E:H/RL:O/RC:C)

Punteggio VPR

9.7

Punteggio base CVSS v2.0

9.3 (CVSS2#AV:N/CA:M/Au:N/DO:DO/MI:DO/LA:DO)

Punteggio temporale CVSS v2.0

8.1 (CVSS2#E:H/RL:OF/RC:C)

STIG Gravità

IO

Riferimenti

OFFERTA	96703
OFFERTA	96704
OFFERTA	96705
OFFERTA	96706
OFFERTA	96707
OFFERTA	96709
CVE	CVE-2017-0143
CVE	CVE-2017-0144
CVE	CVE-2017-0145
CVE	CVE-2017-0146
CVE	CVE-2017-0147
CVE	CVE-2017-0148
MSKB	4012212

MSKB	4012213
MSKB	4012214
MSKB	4012215
MSKB	4012216
MSKB	4012217
MSKB	4012606
MSKB	4013198
MSKB	4013429
MSKB	4012598
XRIF	EDB-ID:41891
XRIF	EDB-ID:41987
XRIF	MSFT:MS17-010
XRIF	IAVA:2017-A-0065
XRIF	CISA-NOTA-SFRUTTATA:2022/05/03
XRIF	CISA-NOTA-SFRUTTATA:2022/08/10
XRIF	CISA-NOTA-SFRUTTATA:2022/04/15
XRIF	CISA-NOTA-SFRUTTATA:2022/04/27
XRIF	CISA-NOTA-SFRUTTATA: 14/06/2022

Sfruttabile con

CANVAS (vero) Core Impact (vero) Metasploit (vero)

Informazioni sul plug-in

Pubblicato: 20/03/2017, Modificato: 25/05/2022

Uscita del plug-in

tcp/445/cifs

Inviato:
00000054ff534d4225000000001803c800000000000000000000000610e9840320000110000000
00ffffffff0000000000000000000000054000000540 00200230000001100005c00500049005000
45005c0000000000

Ricevuto:
ff534d4225050200c09803c8000000000000000000000000000610e98403200001000000

135860 - WMI non disponibile

Sinossi

Impossibile eseguire query WMI sull'host remoto.

Descrizione

WMI (Windows Management Instrumentation) non è disponibile sull'host remoto su DCOM. Le query WMI vengono utilizzate per raccogliere informazioni sull'host remoto, come il suo stato corrente, la configurazione dell'interfaccia di rete, ecc.

Senza queste informazioni, Nessus potrebbe non essere in grado di identificare il software installato o le vulnerabilità di sicurezza esistenti sull'host remoto.

Guarda anche

https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page

Soluzione

n / a

Fattore di rischio

Nessuno

Informazioni sul plug-in

Pubblicato: 21/04/2020, Modificato: 08/06/2023

Uscita del plug-in

tcp/445/cifs

```
Impossibile connettersi allo spazio dei nomi WMI 'root\CIMV2'.
```