**Omschrijving van de vulnerabilities WINDOWS XP**

Critical:

* MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution (921883) (uncredentialed check)

Omschrijving:

* De remote host is kwetsbaar voor een buffer overrun in de 'Server' is een service die kan een aanvaller willekeurige code kan uitvoeren op de host op afstand met 'SYSTEEM' privileges.

Oplossing:

* Windows besturingssysteem updaten

Critical:

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

Omschrijving:

* De externe Windows-host wordt beïnvloed door een beveiligingslek in de 'Server'-dienst ten gevolge van ongepaste behandeling van RPC-aanvragen. Een niet-geverifieerde, externe kwaadwillende kan misbruik maken van dit, via een speciaal ontworpen RPC-verzoek, om willekeurige code uitvoeren met ' Systeembevoegdheden '.

ECLIPSEDWING is een van meerdere vergelijking groep kwetsbaarheden en exploits bekendgemaakt op 2017/04/14 door een groep bekend als de schaduw makelaars.

Oplossing:

* Windows besturingssysteem updaten

Critical:

* MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)

Omschrijving:

* De remote host wordt beïnvloed door een geheugen corruptie beveiligingsprobleem in SMB die kan een aanvaller willekeurige code uitvoeren of een denial of service tegen de remote host uit te voeren.

Oplossing:

* Windows besturingssysteem updaten

Critical:

* MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (uncredentialed check)

Omschrijving:

* Er bestaan meerdere externe code uitvoering beveiligingslekken in Microsoft Server Message Block 1.0 (SMBv1) toe te schrijven aan ongepaste behandeling van bepaalde verzoeken. Een niet-geverifieerde, externe kwaadwillende gebruiker kan misbruik maken van deze beveiligingslekken, via een speciaal ontworpen pakket, willekeurige programmacode uitvoeren. (CVE-2017-0143 CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)
* Een beveiligingsprobleem met vrijgeven van informatie bestaat in Microsoft Server Message Block 1.0 (SMBv1) toe te schrijven aan ongepaste behandeling van bepaalde verzoeken. Een niet-geverifieerde, externe kwaadwillende gebruiker kan misbruik maken van dit, via een speciaal ontworpen pakket, om gevoelige informatie te onthullen. (CVE-2017-0147)
* ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE en ETERNALSYNERGY zijn vier van meerdere vergelijking groep kwetsbaarheden en exploits bekendgemaakt op 2017/04/14 door een groep bekend als de schaduw makelaars.

Oplossing:

* Windows besturingssysteem updaten

High:

* MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution (917159) (uncredentialed check)

Omschrijving:

* De remote host is kwetsbaar voor overloop van de heap in de 'Server'-service dat kan een aanvaller willekeurige code kan uitvoeren op de externe host met ' Systeembevoegdheden '. Naast dit, is de remote host ook beïnvloed door een beveiligingsprobleem met vrijgeven van informatie in SMB kan die toestaan dat een aanvaller verkrijgen van gedeelten van het geheugen van de externe host.

Oplossing:

* Windows besturingssysteem updaten

Medium:

* Microsoft Windows SMB NULL Session Authentication

Omschrijving:

* De remote host is waarop Microsoft Windows wordt uitgevoerd. Het is mogelijk om het met een NULL sessie (dat wil zeggen, geen login of wachtwoord) inloggen. Afhankelijk van de configuratie, is het mogelijk voor een niet-geverifieerde, externe kwaadwillende gebruiker om de invloed van dit onderwerp voor informatie over de externe host.e remote host is kwetsbaar voor overloop van de heap in de 'Server'-service dat kan een aanvaller willekeurige code kan uitvoeren op de externe host met ' Systeembevoegdheden '. Naast dit, is de remote host ook beïnvloed door een beveiligingsprobleem met vrijgeven van informatie in SMB kan die toestaan dat een aanvaller verkrijgen van gedeelten van het geheugen van de externe host.

Oplossing:

* Gelden de volgende registerwijzigingen per de adviezen Technet waarnaar wordt verwezen:
* Reeks: -HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous = 1 -HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess = 1
* Verwijderen BROWSER van: -HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\NullSessionPipes
* Opnieuw opstarten nadat de registerwijzigingen doorgevoerd worden.

Medium:

* SMB Signing Disabled

Omschrijving:

* Ondertekening is niet vereist op de externe SMB-server. Een niet-geverifieerde, externe aanvaller kan misbruik maken van dit gedrag van de man-in-the-middle-aanvallen tegen de SMB-server.

Oplossing:

* Afdwingen bericht ondertekenen in de host-configuratie. Op Windows, dit komt voor in de beleidsinstelling ' Microsoft-netwerkserver: servercommunicatie digitaal ondertekenen (altijd)'. Op Samba heet de instelling 'server ondertekening'. Zie de koppelingen 'Zie ook' voor verdere details.

**Omschrijving van de vulnerabilities METASPLOITIBLE OS**

Critical:

* Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Omschrijving:

* De SSH host-sleutel is gegenereerd op een Debian of Ubuntu systeem bevat een bug in de random number generator van de OpenSSL-library. Het probleem is te wijten aan een Debian packager het verwijderen van bijna alle bronnen van de entropie in de externe versie van OpenSSL. Een aanvaller kan gemakkelijk verkrijgen van de private deel van de afstandsbediening ingedrukt en gebruik deze om tot het ontcijferen van de externe sessie of het opzetten van een man in the middle ' - aanval.

Oplossing:

* Overweeg alle cryptografische materiaal gegenereerd op de externe host om te raden. Particuliar moeten alle SSH, SSL en OpenVPN sleutelmateriaal opnieuw gegenereerd.

Critical:

* rexecd Service Detection

Omschrijving:

* De rexecd-service wordt uitgevoerd op de externe host. Deze service is ontworpen om te kunnen gebruikers van een netwerk op afstand commando's uitvoeren. Rexecd verstrekt niet echter goede manier van verificatie, zodat het kan worden misbruikt door een aanvaller voor het scannen van een externe host.

Oplossing:

* Commentaar uit de "exec"-regel in /etc/inetd.conf en herstart de inetd proces.

Critical:

* VNC Server 'password' Password

Omschrijving:

* De VNC-server draait op de remote host is beveiligd met een zwak wachtwoord. Nessus kon aan login gebruikend VNC authenticatie en een wachtwoord 'wachtwoord'. Een externe, niet-geverifieerde aanvaller kan misbruik maken van dit te misbruiken, controle van het systeem.

Oplossing:

* De dienst VNC met een sterk wachtwoord te beveiligen.