Vulnerabilidad Accesible SMB

(SMB: Server Message Block)

1. INTRODUCCIÓN

SMB es un protocolo de red que permite a una aplicación o al usuario de una aplicación compartir archivos, discos, directorios, impresoras, puertos seriales y mail slots, a través de una red que usa el sistema operativo Microsoft Windows.

SMB se define como la estructura cliente-servidor, donde el cliente formula una solicitud y el servidor envía su respuesta. En otras palabras permite a un cliente leer, crear y modificar archivos de un servidor remoto; para de esta forma poder comunicarse con cualquier servidor, siempre y cuando este configurado para recibir una solicitud de un cliente SMB.

También existe Samba, que es una implementación libre del protocolo SMB con las extensiones de Microsoft y que funciona sobre sistemas operativos GNU/Linux y en otros UNIX.

2. RIESGO

SMB puede permitir a un atacante remoto obtener información confidencial de los sistemas afectados. El puerto 445 ya ha sido utilizado por varios tipos de ataques, incluyendo los gusanos Sasser y Nimda, para esto dicho puerto necesita estar abierto en entornos Windows.

En mayo de 2017, se explotó una vulnerabilidad de software (puerto 445) que permitió al atacante cifrar los archivos del equipo atacado y que fue conocido como Wanna Cry, que aprovechaba una vulnerabilidad en la implementación del protocolo Server Message Block (SMB) de Microsoft. La vulnerabilidad, denominada como CVE-2017-0144 en el catálogo Common Vulnerabilities and Exposures (CVE), se presentó en la versión 1 del servidor SMB (SMBv1), de varias versiones de Microsoft Windows, permitiéndoles a los atacantes ejecutar un código malicioso en el equipo infectado.

El método de infección se realizó a través de spam masivo a direcciones de correo electrónico con un enlace de descarga. Cuando se descarga el archivo adjunto se infecta el equipo con Wanna Cry y la propagación se realiza desde el ordenador infectado y además se rastrea la red LAN en busca de más equipos con la vulnerabilidad MS17-10

para propagar la infección. EternalBlue es el nombre del exploit que le permite a WannaCryptor autoreplicarse y propagarse rápidamente por la red infectada.

3. DETECCIÓN

SMB hace uso principalmente del puerto 445, aunque puede utilizar los puertos TCP: 139 y UDP: 137, 138.

El reporte de "Accesible SMB" se basa en peticiones TCP al puerto 445 de servidores con direcciones IPv4, e identifican los hosts que tienen el servicio en el puerto 445 y el cual es accesible desde Internet. El comando que se utiliza para verificar si el puerto para SMB está abierto es:

nmap -p 445 [IP]

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
vulnerabilidad	Nombre de la vulnerabilidad reportada
direccion_ip	Dirección IP del host
puerto	Puerto desde donde se obtiene la respuesta SSDP
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
as_name	Nombre del ASN
status_EcuCERT	**Estado de la vulnerabilidad** **Online:** vulnerabilidad reportada por Feeds y comprobada por el EcuCERT en el timestamp_EcuCERT **Offline:** Vulnerabilidad reportada por Feeds, pero en el timestamp_EcuCERT no se detectó.
timestamp	Tiempo en la que la IP fue probada en UTC+0
ip	La dirección IP del dispositivo en cuestión
protocol	Protocolo en que proviene la respuesta (siempre TCP)
port	Puerto en que proviene la respuesta (445/TCP)
hostname	DNS Reverso - nombre del dispositivo en cuestión
tag	Siempre será smb
asn	ASN donde el dispositivo en cuestión se encuentra
geo	País donde el dispositivo en cuestión se encuentra
region	Estado / Provincia / Región Administrativa donde el dispositivo se encuentra
city	Ciudad en la que el dispositivo en cuestión se encuentra
naics	Código de sistema de Clasificación Industrial de América del Norte
sic	Código Estándar de Clasificación Industrial

Campo	Descripción
smb_implant	Indica si un “smb-implant” está presente (Y/N)
arch	Si un smb-implant está presente, indica si la arquitectura del sistema es 32-bit (x86) o 64-bit (x64)
key	Si un smb-implant está presente, indica la cripto llave

4. ACCIONES RECOMENDADAS

- Deshabilitar el puerto 445 en el firewall a menos que de verdad se necesite por algún servicio.

- Aplicar parches de seguridad de Windows, que incluyen la solución al problema de Wanna Cry a través del parche de seguridad MS17-010, para todas las versiones de Windows que en ese momento eran mantenidas por la compañía: Windows Vista, Windows 7, Windows 8.1, Windows 10, Windows Server 2008, Windows Server 2012, y Windows Server 2016. Después de que se produjo el ataque WannaCry que empleaba EternalBlue, Microsoft aportó la actualización de seguridad para Windows XP, Windows 8, y Windows Server 2003, todas disponible para descarga en el Microsoft Update Catalog.

5. REFERENCIAS

- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0016
- http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
- https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4488-informe-del-ransomware-de-la-familia-wannacry-que-incluye-medidas-para-su-deteccion-y-desinfeccion.html
- https://es.wikipedia.org/wiki/Server_Message_Block
- https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2169-ccn-cert-id-17-17-codigo-danino-wannacry-1/file.html