SERVIDORES WINDOWS

AUTOR: RICARDO CASTILLO

NOVIEMBRE: 2020

San Marcos

Introducción

Se han hecho públicos los detalles de explotación de esta vulnerabilidad que afecta de forma directa a los controladores de dominio (DC) del Directorio Activo (AD). Debido a un error en la implementación criptográfica del protocolo Netlogon, específicamente en el uso del cifrado AES-CFB8, es posible establecer una nueva contraseña en el DC. Tras ello, un atacante podría utilizar esa nueva contraseña para tomar el control completo del DC y usurpar las credenciales de un usuario administrador del dominio.

Debido a un uso incorrecto en la implementación del algoritmo de cifrado AES, es posible obtener el control del DC y establecer una contraseña vacía en el dominio. Microsoft lanzó las correspondientes actualizaciones para corregir esta vulnerabilidad, la cual ha sido denominado “Zerologon” debido a la ausencia total de autenticación a la hora de explotarla.

A continuación, se exponen los detalles técnicos de dicha vulnerabilidad.

Contenido

Servidores Windows

Comprometiendo un servidor

Un nuevo fallo crítico afecta todas las versiones de Windows Server configuradas como Controlador de Dominio (DC) con Active Directory (AD).

Microsoft Windows Server 2008 R2:
Sistemas de 64 bits Service Pack 1 y Server Core installation.
Microsoft Windows Server:
2012 Server Core installation.
2012 R2 Server Core installation.
2016 Server Core installation.
2019 Server Core installation.

Se trata de una vulnerabilidad de elevación de privilegios en el servicio Netlogon en Windows.

La razón por la que este exploit es tan grave es porque permite a los atacantes ganar control instantáneo del Directorio Activo de Windows, y a partir de ahí básicamente pueden hacer lo que quieran con toda la red de ordenadores de una organización o empresa.

La vulnerabilidad CVE-2020-1472

Esta vulnerabilidad es calificada como critica. Aunque Microsoft ya publicó un parche para mitigar el fallo, la empresa está haciéndolo en dos partes, y aun no hay evidencia de que haya sido explotado, pese a que múltiples firmas de seguridad han creado pruebas de concepto en las que muestran cómo es posible usar el parche de Microsoft para trabajar de forma inversa y desarrollar un exploit, lo cierto es que su uso no ha sido generalizado.

Para los menos entendidos, el Directorio Activo o "Active Directory" de Windows es un servicio del sistema operativo para implementar el conjunto de aplicaciones que organizan y almacenan todos los recursos de una red de computadores.
El Directorio Activo es básicamente la barrera que protege todas las máquinas

conectadas a una red, sin embargo, tiene la vulnerabilidad de que solo requiere que un atacante ponga un pequeño pie dentro de la red objetivo para hacerse con todos los privilegios.

Por ejemplo, si un empleado es engañado y termina instalando malware en su ordenador, aunque este no tenga privilegios elevados, su dispositivo una vez comprometido, puede usarse para acceder al resto de la red.

Aunque esto suele ser bastante difícil, investigadores de seguridad de Secura han publicado un informe describiendo el exploit "Zerologon" mostrando cómo cualquier atacante de la red local (como un infiltrado malintencionado o alguien que simplemente conectó un dispositivo a un puerto de red local) puede comprometer completamente el dominio de Windows.

"El atacante no necesita ninguna credencial de usuario". Secura reportó la vulnerabilidad a Microsoft y dicen haber desarrollado un exploit que funciona, pero dado el riesgo que representa no lo han liberado hasta que estén seguros de que los parches de Microsoft han sido instalados en la mayoría de los servidores vulnerables.

Null sessions

Una sesión nula es un inicio de sesión en una red utilizando una identidad anónima que permite al usuario ver una lista de recursos disponibles en la red. Esto funciona a través de un recurso compartido conocido como comunicación entre procesos (IPC $) en computadoras con Windows. Muchos sistemas operativos Windows vienen con sesiones nulas habilitadas de manera predeterminada, y algunas permiten a los usuarios desactivar esta función si tienen dudas sobre la seguridad y no hay razón para dejarla habilitada.

Hay varios problemas de seguridad con una conexión de sesión nula. Una es que puede permitir a un hacker acceso de lectura / escritura en las computadoras de la red. Esto se puede usar para insertar código malicioso y otros materiales en computadoras sin contraseñas. El hacker también puede tomar la lista de recursos y nombres de usuario generados e intentar descifrar las contraseñas; incluso con protección por contraseña, si el pirata informático puede descubrir la contraseña, será posible hacer daño durante una sesión nula.

En las redes universitarias en particular, las sesiones nulas pueden ser una amenaza de seguridad significativa y pueden causar problemas en el departamento de tecnología de la información (TI). Los estudiantes universitarios podrían no asegurar sus recursos en absoluto o podrían usar contraseñas obvias que sean fáciles de adivinar. Después de que las computadoras están infectadas con gusanos, virus y otros materiales, pueden infectar toda la red, creando un brote de problemas informáticos. Las computadoras seguras que contienen datos confidenciales podrían estar conectadas a la red, por lo que esto podría conducir a la divulgación de información privada, como los registros de los estudiantes, si un pirata informático está particularmente determinado.

La conexión anónima permite a un pirata informático espiar las actividades que están ocurriendo en la red. Los miembros del personal de tecnología de la información (TI) podrán ver la sesión nula si inician sesión para mirar a los usuarios, y algunos sistemas de seguridad están configurados para alertar cuando alguien parece estar escaneando una red con dicha sesión. Aunque una sesión nula puede tener usos válidos y completamente legales, estos pueden ser lo suficientemente limitados como para que las computadoras conectadas a una red puedan configurarse para no permitir tales conexiones por razones de seguridad.

Conclusiones y recomendaciones

En conclusión, como una solución temporal hasta la aplicación del parche, los investigadores y Microsoft sugieren establecer la longitud máxima de un mensaje DNS (sobre TCP) en 0xFF00, lo que debería aminorar la vulnerabilidad. No es la solución más eficaz, pero por el momento se debe contemplar como una posibilida, debido a que, por el momento, Microsoft no ha publicado medidas de mitigación alternativas en caso de no ser posible aplicar los parches oficiales lanzados el pasado mes de agosto. No obstante, Microsoft ya ha anunciado que para el 2021 publicará nuevas actualizaciones que abordarán de mejor manera la solución a este error. Por lo tanto, es vital implementar las actualizaciones descritas en este aviso en cuanto sea posible dado el gran impacto que puede ocasionar un ataque que explote con éxito esta vulnerabilidad, al tratarse de una tecnología ampliamente extendida a nivel empresarial y teniendo en cuenta el enorme beneficio que puede obtener un atacante.

Referencias bibliográficas

- Genbeta (2020) La última vulnerabilidad en Windows Sever permite tomar control instantáneo sobre toda la red de ordenadores de una empresa. Recuperado de: https://www.genbeta.com/windows/ultima-vulnerabilidad-windows-sever-permite-tomar-control-instantaneo-toda-red-ordenadores-empresa

- Netinbag (2020) ¿Qué es una sesión nula? Recuperado de: https://www.netinbag.com/es/internet/what-is-a-null-session

- Incibe (2020). Vulnerabilidad crítica del protocolo NetLogon en las versiones Windows Server. Recuperado de https://www.incibe.es/protege-tu-empresa/avisos-seguridad/vulnerabilidad-critica-del-protocolo-netlogon-las-versiones

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica