Actualizacion Vulnerabilidad Crítica Microsoft Windows SMBv3

Microsoft reveló el martes una falla grave en Windows SMB_v3 que podría ser explotada por los atacantes para tomar el control de clientes y servidores vulnerables de forma remota. Abreviatura del bloque de mensajes del servidor, SMB es un protocolo utilizado por Windows para compartir archivos, impresoras, puertos serie, comunicaciones y más entre sistemas.

Descripción

Microsoft está desarrollando un parche para la vulnerabilidad crítica, aún no hay una solución completa disponible. Como resultado, recomienda que todos los administradores de Windows instalen inmediatamente soluciones alternativas para evitar que los hackers exploten la falla en los servidores SMB.

Pero no existen soluciones alternativas para clientes SMB."Microsoft es consciente de una vulnerabilidad de ejecución remota de código en la forma en que el protocolo Microsoft Server Message Block 3.1.1 (SMBv3) maneja ciertas solicitudes", dice Microsoft en su alerta de seguridad. "Un atacante que aprovechó con éxito la vulnerabilidad podría obtener la capacidad de ejecutar código en el servidor SMB o cliente SMB de destino".El aviso agrega: "Puede deshabilitar la compresión para impedir que los atacantes no autenticados aprovechen la vulnerabilidad contra un servidor SMBv3".La falla existe en todas las versiones de Windows 10, así como en Windows Server Core, compilaciones 1903 y 1909. No está claro si alguna versión de Windows que ya no sea compatible también podría verse afectada."Para aprovechar la vulnerabilidad contra un servidor SMB, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 específico.

Para aprovechar la vulnerabilidad contra un cliente SMB, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él.

Sistemas operativos afectados

• Windows 10 versión 1903 para sistemas de 32 bits
• Windows 10 versión 1903 para sistemas basados en ARM64
• Windows 10 versión 1909 para sistemas de 32 bits
• Windows 10 versión 1909 para sistemas basados en ARM64
• Windows 10 versión 1909 para sistemas basados en x64
• Windows Server, versión 1903 (Instalación Server Core)
• Windows Server, versión 1909 (Instalación Server Core)

Actualmente, no hay parches disponibles para esta vulnerabilidad. Sin embargo, Microsoft ha proporcionado soluciones en un aviso de seguridad: deshabilite la compresión SMBv3 y bloquee el puerto TCP 445 en las computadoras cliente y los firewalls para evitar que los atacantes aprovechen la vulnerabilidad.

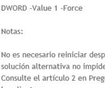
Detección de CVE-2020-0796 con Qualys VM

Qualys ha emitido QID 91614 para Qualys Vulnerability Management que cubre CVE-2020-0796 en todos los sistemas operativos afectados.

Este QID se incluirá en la versión de firma VULNSIGS-2.4.837-4, y requiere escaneo autenticado o Qualys Cloud Agent.

Los agentes en la nube recibirán automáticamente este nuevo QID como parte de la versión de manifiesto 2.4.837.4-3.

Los detalles de la detección también están disponibles en Microsoft Security Alert: 10 de marzo de 2020.QID 91614: Guía de Microsoft para deshabilitar la compresión SMBv3 no aplicada (ADV200005)



Este QID comprueba si SMBv3 está habilitado en el host y si no se aplica la siguiente solución:

"HKLM SYSTEM CurrentControlSet Services LanmanServer Parameter"DisableCompression -Type DWORD -Value 1

Puede buscar esto dentro de VM Dashboard mediante la siguiente consulta

QQL:vulnerabilidades.vulnerability.cveIds: CVE-2020-0796vulnerabilidades.vulnerability.qid: 91614

Mitigaciones disponibles CVE-2020-0796

Para proteger a los clientes contra ataques transmitidos por Internet, la "mejor defensa" es bloquear el puerto TCP 445, que "se utiliza para iniciar una conexión con el componente afectado en el firewall del perímetro de la red ayudará a proteger los sistemas que están detrás de ese firewall de los intentos de explotar esta vulnerabilidad.

En la mayoría de los casos, la vulnerabilidad de SMB se limitará a las redes internas. Sin embargo, es clave asegurarse de que no está exponiendo el servicio a Internet

Microsoft publica los parches para mitigacion de la vulnerabilidad

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796

Mitigaciones

Microsoft no ha identificado ningún factor atenuante para esta vulnerabilidad.Soluciones

La siguiente solución puede ser útil en su situación. En todos los casos, Microsoft recomienda encarecidamente que instale las actualizaciones para esta vulnerabilidad tan pronto como estén disponibles, Incluso si planea dejar esta solución alternativa en su lugar:

Deshabilitar la compresión SMBv3

Puede deshabilitar la compresión para impedir que los atacantes no autenticados aprovechen la vulnerabilidad contra un servidor SMBv3 con el siguiente comando de PowerShell.

Set-itemProperty -Path "HKLM: SYSTEM CurrentControlSet Services LanmanServer Parameters" DisableCompression -Type DWORD -Value 1 -Force

Notas:

No es necesario reiniciar después de realizar el cambio. Esta solución alternativa no impide la explotación de clientes SMB; Consulte el artículo 2 en Preguntas frecuentes para proteger a los clientes.

Puede deshabilitar la solución alternativa con el siguiente comando de PowerShell.Set-ItemProperty -Path "HKLM: SYSTEM CurrentControlSet Services LanmanServer Parameters" DisableCompression -Type DWORD -Value 0 -Force

Nota:

No es necesario reiniciar después de deshabilitar la solución.

Referencias:

https://www.bleepingcomputer.com/news/security/microsoft-leaks-info-on-wormable-windows-smbv3-cve-2020-0796-flaw/

https://thehackernews.com/2020/03/smbv3-wormable-vulnerability.htmlhttps://arstechnica.com/information-technology/2020/03/windows-has-a-new-wormable-vulnerability-and-theres-no-patch-in-sight/

https://blog.qualys.com/laws-of-vulnerabilities/2020/03/11/microsoft-windows-smbv3-remote-code-execution-vulnerability-cve-2020-0796

https://www.bankinfosecurity.com/windows-alert-critical-smbv3-flaw-requires-workaround-a-13922

Empresa Afectada:
Microsoft
Publicación:
12/03/2020
Importancia:
Alta
Riesgo de explotación:
Alta
Tipo de explotación:
Remoto

Fuentes:

Qualys
Microsoft

Recomendaciones

- Ejecutar programas de concientización al personal sobre los últimos ataquesde phishing / spearphishing
- No hacer click a links en correos sospechosos yno confiar en correos de remitentes des conocidos.
- Actualización de firmas de antivirus y parchesde sistema operativo.
- Mantener configurado el SPF del dominio de correo. Al hacerlo, restringir los privilegios de los usuarios paralinstalar y ejecutar aplicaciones en las máquinas de la organización, usando elprincipio de mínimo privilegio.
- Limitar los privilegios para procesos desconocidos,escribiendo reglas para HIPS (sistemas de prevención de intrusiones de host) oreglas de protección de acceso.