Microsoft lanzó finalmente una actualización de software de emergencia para parchear la vulnerabilidad crítica recientemente revelada en el protocolo SMBv3, que podría permitir a los atacantes lanzar malware malicioso, que puede propagarse automáticamente de una computadora a otra.

La vulnerabilidad, rastreada como CVE-2020-0796, es un error de ejecución remota de código que afecta a Windows 10 versión 1903 y 1909, y Windows Server versión 1903 y 1909.

Server Message Block (SMB), que se ejecuta sobre el puerto TCP 445, es un protocolo de red que fue diseñado para permitir el intercambio de archivos, la navegación en red, los servicios de impresión y la comunicación entre procesos por medio de una red.

La última vulnerabilidad, para la que existe una actualización de parche (KB4551762) disponible en el sitio web de Microsoft, existe en la forma en que el protocolo SMBv3 maneja las solicitudes con encabezados de compresión, lo que hace posible que los atacantes remotos no autenticados ejecuten código malicioso en servidores o clientes objetivo con privilegios de SISTEMA.

Los encabezados de compresión son una característica que se agregó al protocolo afectado de los sistemas operativos Windows 10 y Windows Server en mayo de 2019, diseñado para comprimir el tamaño de los mensajes intercambiados entre un servidor y los clientes conectados a él.

> *«Para explotar la vulnerabilidad contra un servidor, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 específico. Para explotar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte»,* dijo Microsoft.

Hasta el momento, solo existe un exploit PoC conocido para la falla crítica explotable remotamente, pero la ingeniería inversa de nuevos parches ahora también podría ayudar a

los hackers a encontrar posibles vectores de ataque para el desarrollo de malware autopropagante totalmente armado.

Un equipo separado de investigadores también ha publicado un análisis técnico detallado de la vulnerabilidad, concluyendo un desbordamiento de kernel como la causa raíz del problema.

Existen casi 48 mil sistemas Windows vulnerables a la última vulnerabilidad de compresión SMB y accesibles por medio de Internet.

Debido a que ahora se puede descargar un parche para la falla SMBv3 que se puede eliminar para las versiones afectadas en Windows, es muy recomendable que los usuarios domésticos y las empresas instalen actualizaciones lo más pronto posible, en lugar de limitarse a confiar en la mitigación.