Al poco tiempo después de la liberación del lote mensual de actualizaciones de seguridad, Microsoft emitió ayer por la tarde por separado, un asesoramiento a sus mil millones de usuarios de Windows sobre una nueva vulnerabilidad crítica, sin parches, que afecta a Server Message Block 3.0 (protocolo de comunicación SMBv3).

Parece ser que Microsoft planeó en un principio, corregir la falla como parte de su actualización del martes de marzo de 2020, pero por alguna razón, no se logró este objetivo.

La vulnerabilidad CVE-2020-0796, de ser explotada con éxito, podría permitir que un hacker ejecute código arbitrario en el servidor SMB o cliente SMB de destino. Investigadores han denominado al error como SMBGhost.

> *«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»*, dijo Microsoft.

El protocolo de bloqueo de mensajes del servidor proporciona la base para compartir archivos, navegar por la red, servicios de impresión y comunicación entre procesos de una red.

Según una publicación de Cisco Talos ahora eliminada, la falla abre los sistemas vulnerables a un ataque «*wormable*», lo que facilita la propagación entre víctimas.

No está claro todavía cuándo Microsoft corregirá la falla, pero la compañía pide a los usuarios que deshabiliten la compresión SMBv3 y bloqueen el puerto TCP 445 en firewalls y computadoras cliente como una solución alternativa.

Set-ItemProperty -Path «HKLM: \ SYSTEM \ CurrentControlSet \ Services \ LanmanServer \ Parameters» DisableCompression -Type DWORD -Value 1 -Force

Además, Microsoft advirtió que deshabilitar la compresión SMBv3 no impedirá la explotación de clientes SMB.

Cabe señalar que la falla solo afecta a Windows 10 versión 1903, Windows 10 versión 1909, Windows Server versión 1903 y Windows Server versión 1909. Pero es posible que se vean afectadas más versiones ya que SMB 3.0 se introdujo con Windows 8 y Windows Server 2012.

A pesar de la gravedad del error SMB, no existe evidencia de que se esté explotando en la naturaleza. Pero también es necesario llamar la atención sobre el hecho de que esto está lejos de ser la única vez que SMB ha sido explotado como un vector de ataque para intentos de intrusión.

En los últimos años, algunas de las principales infecciones de ransomware, incluyendo WannaCry y NotPetya, fueron consecuencia de exploits basados en SMB.

Mientras tanto, hasta que Microsoft lance una actualización de seguridad diseñada para corregir la falla CVE-2020-0796 RCE, se recomienda a los administradores de sistemas que implementen soluciones para bloquear los ataques que intentan aprovechar la vulnerabilidad.