Investigadores de seguridad cibernética descubrieron hoy una nueva vulnerabilidad crítica que afecta el protocolo Server Message Block (SMB), que podría permitir que los hackers pierdan la memoria del núcleo de forma remota, y al combinar con un error *«wormable»* previamente divulgado, la falla puede ser explotada para lograr ataques de ejecución remota de código.

Nombrado *«SMBleed»* (CVE-2020-1206), por la compañía de seguridad ZecOps, el defecto reside en la función de descompresión de SMB, la misma función que con el error SMBGhost o EternalDarkness (CVE-2020-0796), que se dio a conocer hace tres meses, potencialmente abriendo sistemas vulnerables de Windows a ataques de malware que pueden propagarse mediante redes.

La vulnerabilidad recién descubierta afecta las versiones de Windows 10 1903 y 1909, para las cuales Microsoft lanzó hoy parches de seguridad como parte de sus actualizaciones mensuales de Patch Tuesday para junio de 2020.

El desarrollo se produce cuando la Agencia de Seguridad de Infraestructura y Cibersegurdad de Estados Unidos (CISA), emitió un aviso la semana pasada advirtiendo a los usuarios de Windows 10 que actualicen sus máquinas luego de que el código de explotación para el error SMBGhost se publicara en línea la semana pasada.

SMBGhost se consideró tan grave que recibió la puntuación máxima de 10.

> *«Aunque Microsoft reveló y proporcionó actualizaciones para esta vulnerabilidad en marzo de 2020, los actores maliciosos están apuntando a sistemas no parcheados con el nuevo PoC, según informes recientes de código abierto»*, dijo CISA.

SMB, que se ejecuta sobre el puerto TCP 445, es un protocolo de red que proporciona la base para compartir archivos, navegar por la red, servicios de impresión y comunicación entre procesos a través de una red.

Según los investigadores de ZecOps, la falla se debe a la forma en que la función de descompresión en cuestión «Srv2DecompressData» maneja las solicitudes de mensajes especialmente diseñados enviados a un servidor SMBv3 de destino, lo que permite a un atacante leer la memoria del núcleo no inicializada y realizar modificaciones en la función de compresión.

> *«La estructura del mensaje contiene campos como la cantidad de bytes para escribir y marcar, seguidos de un búfer de longitud variable. Eso es perfecto para explotar el error, ya que podemos crear un mensaje que especifique el encabezado, pero el búfer de longitud variable contiene datos no inicializados»,* dijeron los investigadores.
>
> *«Un atacante que explotó exitosamente la vulnerabilidad, podría obtener información para comprometer aún más el sistema del usuario. Para explotar la vulnerabilidad contra un servidor, un atacante no autenticado podría enviar un paquete especialmente diseñado a un servidor SMBv3 específico»*, dijo Microsoft en su aviso.
>
> *«Para aprovechar la vulnerabilidad contra un cliente, un atacante no autenticado necesitaría configurar un servidor SMBv3 malicioso y convencer a un usuario para que se conecte a él».*

SMBleed se puede encadenar con SMBGhost en sistemas Windows 10 sin parches para lograr la ejecución remota de código. La firma también lanzó un código de explotación de prueba de concepto que demuestra los defectos.

Para mitigar la vulnerabilidad, se recomienda que los usuarios domésticos y empresariales instalen las últimas actualizaciones de Windows lo más pronto posible.

Para sistemas donde el parche no es aplicable, se recomienda bloquear el puerto 445 para evitar el movimiento lateral y la explotación remota.

La guía de seguridad de Microsoft acerca de CMBleed y SMBGhost en Windows 10 versiones 1909 y 1903, y Server Core para las mismas versiones, pueden verse aquí y aquí.