SMBGhost, el fantasma de los archivos compartidos

RESUMEN: El SMBGhost es un sistema que afecta al protocolo y lo que hace es permitir compartir archivos e impresoras entre otros servicios en una red.

CATEGORÍAS: CIBERSEGURIDAD

Nº HIPERVINCULOS: 2

SMBGhost es un agujero de seguridad que afecta a algunas versiones de Windows 10 y Windows Server Core.

Este sistema es una amenaza que afecta al protocolo SMBv3 (Server Message Block) y lo que hace es permitir compartir archivos e impresoras entre otros servicios en una red. Su nombre está formado por el protocolo SMB, al que se añade la palabra "Ghost", para indicar que el atacante necesita configurar un servidor SMB y convencer al usuario para que se conecte a él sin que se percate de lo que pasa. Es decir, de forma fantasma.

Además, la vulnerabilidad solo ha sido visible durante un tiempo o por tiempos intermitentes. Puedes consultar los detalles de esta vulnerabilidad en el aviso de "Protege tu empresa".

Versiones anteriores de este protocolo ya habían sufrido otra vulnerabilidad, cuyo exploit, llamado EternalBlue, también permitió a los ciberdelincuentes propagar ransomware, conocido como WannaCry, entre los equipos afectados, provocando importantes consecuencias.

Incibe señala una serie de consejos y recomendaciones para saber cómo actuar en estos casos. En primer lugar, debes saber cuál es la versión de Windows que tienes, si es la 10 o Server Core.

Para ello, no basta con saber si es Pro o Home, sino el número de versión. Esto se puede realizar en Windows 10 de al menos 3 maneras diferentes. La primera, y la más fácil, es presionar la tecla con el logotipo de Windows y la tecla pausa situada en la parte superior del teclado, tras lo cual nos aparecerá una ventana mostrando la información de nuestro sistema. Las otras 2 maneras son similares en la forma y se hacen siguiendo estos sencillos pasos:

- Vamos al símbolo de inicio de Windows (en la esquina inferior izquierda de la pantalla), damos al botón derecho del ratón y hacemos clic sobre 'Ejecutar'.
- En la ventana que se abre podemos teclear uno de estos comandos: «winver» o «msinfo32.exe», y pulsar el botón 'Aceptar'.
  - Si hemos tecleado «winver», a continuación, se nos abrirá una ventana con la información de nuestro sistema similar a la mostrada debajo.
  - Si por el contrario hemos optado por «msinfo32», en 'Resumen del sistema', a la derecha, veremos 'Nombre del SO' (sistema operativo), e inmediatamente debajo, la versión del sistema instalada, como en la imagen mostrada a continuación.

Si tu sistema tiene la versión 1903 o 1909, debes actualizar cuanto antes para aplicar la protección contra esta vulnerabilidad. Si tu versión es diferente, puedes estar tranquilo, ya que esta vulnerabilidad solo afecta a las versiones mencionadas.

Por otro lado, si aún no tienes activadas las actualizaciones automáticas en tus dispositivos o ni siquiera lo sabes, ahora es el momento de ponerle solución y verificar este punto. Te llevará un minuto y te ayudará a estar tranquilo. Así, tu equipo estará protegido contra posibles incidentes de este tipo. Además, los ciberdelincuentes prefieren atacar equipos desprotegidos, más fáciles y rápidos de comprometer.