BOLETÍN DE ALERTA

Boletín Nro.: 2022-54
Fecha de publicación: 27/12/2022
Tema: Múltiples vulnerabilidades del *kernel* de Linux afectan a los servidores SMB.

Los productos afectados son:

- *Kernel* de Linux, versión 5.15 hasta 5.19, anteriores a 5.19.2.
- *Kernel* de Linux, versión 5.15 hasta 5.18, anteriores a 5.18.18.

Descripción:

Se ha reportado un nuevo aviso de seguridad sobre cinco vulnerabilidades que afectan al componente *ksmbd* y *CIFS* del *kernel* Linux, que permitirían a un atacante realizar ejecución arbitraria de código, denegación de servicios (*DoS*), entre otros.

Las vulnerabilidades reportadas se componen de 2 (dos) de severidad "Crítica", 1 (una) de severidad "Alta" y 2 (dos) de severidad "Media". Las principales se detallan a continuación:

- CVE-2022-47939, de severidad "crítica" y con puntuación asignada de 10.0. Esta vulnerabilidad del tipo *use-after-free* (*UAF*) se debe a una falla en la validación de entrada al procesar el comando *SMB2_TREE_DISCONNECT*. Esto permitiría a un atacante remoto realizar ejecución arbitraria de código en el sistema afectado.

- CVE-2022-47940, de severidad "crítica" y con puntuación asignada de 9.6. Esta vulnerabilidad de lectura fuera de los límites se debe a la falta de validación correcta de entrada de datos del usuario al utilizar el comando *SMB2_WRITE*. Esto permitiría a un atacante remoto y autenticado realizar divulgación de información confidencial.

- CVE-2022-47942, de severidad "alta" y con puntuación asignada de 8.5. Esta vulnerabilidad de desbordamiento de *buffer* se debe a una falla en la validación de entrada de los datos proporcionados por el usuario. Esto permitiría a un atacante remoto realizar ejecución arbitraria de código en el sistema afectado.

Puede acceder a la lista completa de las vulnerabilidades en el siguiente enlace.

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante ejecutar código arbitrario, divulgar información confidencial, entre otros.

Solución:

Recomendamos acceder a la actualización de seguridad correspondiente a través de los siguientes enlaces:

- https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61
- https://lore.kernel.org/lkml/20220819153711.816369367@linuxfoundation.org/
- https://lore.kernel.org/lkml/20220819153711.847846093@linuxfoundation.org/
- https://lore.kernel.org/lkml/20220819153711.847846093@linuxfoundation.org/

Información adicional:

- https://www.zerodayinitiative.com/advisories/ZDI-22-1690/
- https://access.redhat.com/solutions/6991749
- https://nvd.nist.gov/vuln/detail/CVE-2022-47939
- https://nvd.nist.gov/vuln/detail/CVE-2022-47940
- https://nvd.nist.gov/vuln/detail/CVE-2022-47942
- https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61
- https://lore.kernel.org/lkml/20220819153711.816369367@linuxfoundation.org/
- https://lore.kernel.org/lkml/20220819153711.847846093@linuxfoundation.org/
- https://lore.kernel.org/lkml/20220819153711.847846093@linuxfoundation.org/