Se han revelado detalles sobre una reciente vulnerabilidad de seguridad identificada en el núcleo de Linux que podría permitir a un usuario obtener privilegios elevados en un host objetivo.

Conocida como StackRot (CVE-2023-3269, puntuación CVSS: 7.8), esta falla afecta a las versiones de Linux 6.1 hasta 6.4. Hasta ahora, no se ha encontrado evidencia de que esta debilidad haya sido explotada en la práctica.

Según Ruihan Li, investigador de seguridad de la Universidad de Pekín, *«Dado que StackRot es una vulnerabilidad en el kernel de Linux que se encuentra en el subsistema de gestión de memoria, afecta prácticamente a todas las configuraciones del kernel y requiere capacidades mínimas para ser activada»*.

> *«No obstante, es importante tener en cuenta que los nodos de maple se liberan mediante devoluciones de llamada de RCU, lo que retrasa la desasignación real de memoria hasta después del período de gracia de RCU. En consecuencia, aprovechar esta vulnerabilidad se considera un desafío».*

Tras una divulgación responsable el 15 de junio de 2023, el problema ha sido abordado en las versiones estables 6.1.37, 6.3.11 y 6.4.1 a partir del 1 de julio de 2023, después de un esfuerzo de dos semanas liderado por Linus Torvalds.

Se espera que, para finales de mes, se haga pública una prueba de concepto (PoC) y detalles técnicos adicionales sobre el error.

Fundamentalmente, esta falla tiene su origen en una estructura de datos denominada árbol de maple, que se introdujo en el kernel de Linux 6.1 para reemplazar al árbol rojo-negro (rbtree) y así gestionar y almacenar áreas de memoria virtual (VMAs). Estas VMAs son rangos contiguos de direcciones virtuales que pueden representar el contenido de un archivo en disco o la memoria utilizada por un programa durante su ejecución.

En términos específicos, se trata de un error de uso después de liberar la memoria que podría ser explotado por un usuario local para comprometer el kernel y aumentar sus privilegios, aprovechando el hecho de que el árbol de maple *«puede experimentar el reemplazo de nodos sin adquirir correctamente el bloqueo de escritura MM».*

> De todas formas, Torvalds mencionó: *«En cualquier caso, creo que quiero trasladar todo el código de expansión de la pila a un archivo completamente nuevo, en lugar de tenerlo dividido entre mm/mmap.c y mm/memory.c. Sin embargo, dado que esto deberá ser adaptado a la introducción inicial del árbol de maple VMA, he tratado de mantener los parches lo más mínimos posible».*