Microsoft ha revelado detalles sobre una vulnerabilidad de seguridad en macOS de Apple que ya ha sido corregida. Esta falla podría haber permitido a un atacante, actuando como «root», evitar la Protección de Integridad del Sistema (SIP) del sistema operativo e instalar controladores de kernel maliciosos al cargar extensiones de kernel de terceros.

La vulnerabilidad, identificada como CVE-2024-44243 (con una puntuación CVSS de 5.5), es un error de severidad media que Apple resolvió en la actualización de macOS Sequoia 15.2, publicada el mes pasado. Según Apple, se trataba de un *«problema de configuración»* que podía permitir que una aplicación maliciosa alterara partes protegidas del sistema de archivos.

> *«Superar las protecciones de SIP puede tener consecuencias graves, como facilitar que atacantes y desarrolladores de malware instalen rootkits, generen software malicioso persistente, evadan las políticas de Transparencia, Consentimiento y Control (TCC) y aumenten las posibilidades de usar otras técnicas y exploits»*, explicó Jonathan Bar Or, del equipo de inteligencia de amenazas de Microsoft.

SIP, también conocido como «rootless», es un sistema de seguridad diseñado para evitar que el software malintencionado modifique áreas críticas del sistema operativo, como las carpetas /System, /usr, /bin, /sbin, /var y las aplicaciones preinstaladas.

Este sistema se basa en imponer restricciones incluso al usuario root, permitiendo cambios en estas áreas únicamente a procesos firmados por Apple que cuentan con permisos específicos para modificar archivos del sistema, como las actualizaciones de software e instaladores oficiales de Apple.

Los principales derechos que habilitan estas modificaciones dentro de SIP son:

- com.apple.rootless.install, que elimina las restricciones del sistema de archivos para un proceso autorizado.
- com.apple.rootless.install.heritable, que extiende estas autorizaciones a un proceso y

todos sus procesos secundarios que heredan este derecho.

La vulnerabilidad CVE-2024-44243, descubierta por Microsoft, aprovecha el derecho «com.apple.rootless.install.heritable» asociado al demonio Storage Kit (storagekitd) para eludir las protecciones de SIP. Esta es la última de una serie de fallas similares detectadas por Microsoft, como CVE-2021-30892 (Shrootless) y CVE-2023-32369 (Migraine).

El exploit funciona explotando *«la capacidad de storagekitd para ejecutar procesos arbitrarios sin validaciones adecuadas o reducciones de privilegios».* Esto permite colocar un nuevo paquete en /Library/Filesystems, un proceso hijo de storagekitd, y sobrescribir binarios relacionados con la Utilidad de Discos, que podrían activarse en operaciones específicas como la reparación de discos.

> *«Un atacante con acceso root puede agregar un nuevo paquete al sistema de archivos en /Library/Filesystems y luego usar storagekitd para ejecutar binarios personalizados, eludiendo así SIP. Realizar una operación de borrado en el nuevo sistema de archivos creado también permite evadir estas protecciones»,* afirmó Bar Or.

Este descubrimiento llega apenas tres meses después de que Microsoft revelara otra vulnerabilidad en el marco de Transparencia, Consentimiento y Control (TCC) de macOS, conocida como HM Surf (CVE-2024-44133, puntuación CVSS: 5.5), que podría ser utilizada para acceder a información sensible.

> *«Restringir la ejecución de código de terceros en el kernel puede mejorar la estabilidad de macOS, aunque a costa de limitar las capacidades de monitoreo de las soluciones de seguridad»,* señaló Bar Or.
>
> *«Si SIP se vulnera, todo el sistema operativo pierde su confiabilidad. Además, con*

> *una menor visibilidad de monitoreo, los atacantes podrían manipular las herramientas de seguridad en el dispositivo para evitar ser detectados».*