Investigadores en ciberseguridad han demostrado un prototipo funcional (PoC) de un *rootkit* llamado Curing, que aprovecha un mecanismo de entrada/salida asíncrona en Linux llamado io_uring para evadir la monitorización tradicional de llamadas al sistema.

Según la empresa ARMO, esto representa un *«punto ciego importante en las herramientas de seguridad en tiempo de ejecución de Linux».*

En su informe, ARMO explica:

> *"Este mecanismo permite que una aplicación de usuario realice varias acciones sin depender de las llamadas al sistema. Por lo tanto, las herramientas de seguridad que se basan en la supervisión de dichas llamadas no pueden detectar rootkits que utilicen únicamente io_uring."*

io_uring, introducido por primera vez en la versión 5.1 del núcleo de Linux en marzo de 2019, es una interfaz del sistema que utiliza dos búferes circulares —una cola de envío (*submission queue*) y una cola de finalización (*completion queue*)— para gestionar de forma asíncrona las peticiones de entrada/salida entre el núcleo y las aplicaciones en espacio de usuario.

El *rootkit* desarrollado por ARMO establece comunicación entre un servidor de comando y control (*C2*) y el equipo infectado, permitiendo recibir y ejecutar órdenes sin recurrir a las llamadas al sistema, usando en su lugar io_uring para cumplir sus objetivos.

El análisis de ARMO sobre las herramientas de seguridad en tiempo real para Linux muestra que soluciones populares como Falco y Tetragon no son capaces de detectar actividades basadas en io_uring, ya que dependen fuertemente de la interceptación de llamadas al sistema.

Los riesgos de seguridad asociados con io_uring ya eran conocidos. En junio de 2023, Google anunció que restringiría su uso en Android, ChromeOS y sus servidores de producción debido

a que *«ofrece primitivas de explotación muy potentes».*

Amit Schendel, jefe de investigación en seguridad de ARMO, comentó:

> *«Por un lado, necesitas visibilidad sobre las llamadas al sistema; por otro, también necesitas acceso a las estructuras internas del núcleo y al contexto suficiente para detectar amenazas de forma efectiva. Muchos proveedores optan por el camino más fácil: engancharse directamente a las llamadas al sistema. Aunque esta estrategia ofrece visibilidad rápida, tiene limitaciones importantes. La más destacada es que las llamadas al sistema no siempre se usan. io_uring, que puede evitarlas por completo, es un excelente ejemplo de ello.»*