Se ha detectado una nueva vulnerabilidad de seguridad en Linux denominada «*Looney Tunables*» en el cargador dinámico ld.so de la Biblioteca C GNU (glibc). Si se explota con éxito, esta vulnerabilidad podría llevar a una escalada de privilegios locales y permitir que un actor malicioso obtenga privilegios de administrador.

Esta vulnerabilidad, rastreada como CVE-2023-4911 (con una puntuación CVSS de 7.8), es un desbordamiento de búfer que reside en el procesamiento de la variable de entorno GLIBC_TUNABLES por parte del cargador dinámico. La firma de ciberseguridad Qualys, que divulgó detalles sobre esta vulnerabilidad, informó que fue introducida como parte de una modificación de código realizada en abril de 2021.

La Biblioteca C GNU, también conocida como glibc, es una biblioteca fundamental en los sistemas basados en Linux y proporciona funciones esenciales como open, read, write, malloc, printf, getaddrinfo, dlopen, pthread_create, crypt, login y exit.

El cargador dinámico de glibc es un componente crítico que se encarga de preparar y ejecutar programas, lo que incluye la búsqueda de las dependencias de objetos compartidos necesarias y cargarlas en la memoria, así como vincularlas en tiempo de ejecución.

Esta vulnerabilidad afecta a importantes distribuciones de Linux como Fedora 37 y 38, Ubuntu 22.04 y 23.04, y Debian 12 y 13. Es probable que otras distribuciones también sean vulnerables y susceptibles de explotación, aunque una excepción notable es Alpine Linux, que utiliza la biblioteca musl libc en lugar de glibc.

> Saeed Abbasi, gerente de productos de la Unidad de Investigación de Amenazas de Qualys, señaló: *«La presencia de una vulnerabilidad de desbordamiento de búfer en el manejo de la variable de entorno GLIBC_TUNABLES por parte del cargador dinámico plantea riesgos significativos para numerosas distribuciones de Linux. Esta variable de entorno, diseñada para ajustar y optimizar aplicaciones vinculadas con glibc, es una herramienta esencial para desarrolladores y administradores de sistemas. Su uso indebido o explotación tiene un amplio impacto en el rendimiento,*

> *la confiabilidad y la seguridad del sistema».*

Según un aviso emitido por Red Hat, un atacante local podría aprovechar esta vulnerabilidad utilizando variables de entorno GLIBC_TUNABLES especialmente diseñadas al ejecutar binarios con permisos SUID para ejecutar código con privilegios elevados. Red Hat también ha proporcionado una mitigación temporal que, cuando se activa, finaliza cualquier programa con permisos SUID que se invoque con GLIBC_TUNABLES en el entorno.

Looney Tunables se suma a una lista cada vez más larga de vulnerabilidades de escalada de privilegios descubiertas en Linux en los últimos años, incluyendo CVE-2021-3156 (Baron Samedit), CVE-2021-3560, CVE-2021-33909 (Sequoia) y CVE-2021-4034 (PwnKit), que podrían ser utilizadas para obtener permisos elevados.