Alert Bulletin

Bulletin N.:
Publication Date: 19/05/2025
Subject: Alerta 2025-42-Falla crítica en glibc permite ejecutar código malicioso en sistemas Unix
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Bibloteca glibc 2,27 < 2,39

Descripción

Se ha reportado una vulnerabilidad identificada como **CVE-2025-4802 con CVSS 9.8** en la biblioteca GNU C (glibc), un componente esencial en sistemas operativos basados en Unix (como Linux). Esta falla afecta a las versiones 2.27 hasta la 2.38.

El problema se origina en el uso inseguro de la variable de entorno LD_LIBRARY_PATH. Un atacante podría aprovechar esta debilidad para cargar código malicioso en programas privilegiados (binarios setuid) que utilizan ciertas funciones de glibc, como dlopen. Esto podría llevar a la ejecución no autorizada de código, poniendo en riesgo la integridad y seguridad del sistema.

Muchos servidores y dispositivos Linux utilizan glibc, por lo que esta vulnerabilidad podría ser explotada para tomar control de sistemas o acceder a información sensible si no se actualizan.

Solución

Se recomienda a los administradores de sistemas **actualizar glibc 2,39 o una versión corregida tan pronto como esté disponible** y evitar el uso de LD_LIBRARY_PATH en entornos con binarios privilegiados.

Información adicional:

- https://sourceware.org/bugzilla/show_bug.cgi?id=32976
- https://sourceware.org/cgit/glibc/commit/?id=1e18586c5820e329f741d5c710275e165581380e
- https://github.com/advisories/GHSA-8mm9-c4mg-vfjh
- https://securityvulnerability.io/vulnerability/CVE-2025-4802