Se reveló una vulnerabilidad de alta gravedad en la biblioteca de la base de datos SQLite, que se introdujo como parte de un cambio de código que data de octubre de 2000 y podría permitir a los atacantes bloquear o controlar programas.

Rastreada como CVE-2022-35737 (puntaje CVSS: 7.5), el problema de 22 años afecta a las versiones de SQLite 1.0.12 a 3.39.1 y se solucionó en la versión 3.39.2 lanzada el 21 de julio de 2022.

> *«CVE-2022-35737 es explotable en sistemas de 64 bits, y la explotabilidad depende de cómo se compile el programa»,* dijo Andreas Kellas, investigador de Trail of Bits.

> *«La ejecución de código arbitrario se confirma cuando la biblioteca se compila sin canarios de pila, pero no se confirma cuando hay canarios de pila presentes, y la denegación de servicio se confirma en todos los casos».*

Programado en C, SQLite es el motor de base de datos más usado, incluido de forma predeterminada en Android, iOS, Windows y macOS, así como en navegadores web populares como Google Chrome, Mozilla Firefox y Apple Safari.

La vulnerabilidad descubierta por Trail of Bits se refiere a un error de desbordamiento de enteros que ocurre cuando las entradas de cadenas extremadamente grandes se pasan como parámetros a las implementaciones de SQLite de las funciones printf, que a su vez, utilizan otra función para manejar el formato de cadenas («sqlite3_str_vappendf»).

Sin embargo, un armamento exitoso de la falla se basa en el requisito previo de que la cadena contenga los tipos de sustitución de formato %Q, %q o %w, lo que puede provocar un bloqueo del programa cuando los datos controlados por el usuario se escriben más allá de los límites de una pila de búfer asignado.

> *«Si la cadena de formato contiene el caracter especial '!' para habilitar el escaneo de caracteres Unicode, entonces es posible lograr la ejecución de código arbitrario en el peor de los casos, o hacer que el programa se cuelgue y se repita indefinidamente»,* explicó Kellas.

La vulnerabilidad también es un ejemplo de un escenario que alguna vez se consideró poco práctico hace décadas (asignar cadenas de 1 GB como entrada) que se volvió factible con la llegada de los sistemas informáticos de 64 bits.

> *«Es un error que puede no haber parecido un error en el momento en que se escribió (que se remonta a 2000 en el código fuente de SQLite) cuando los sistemas eran principalmente arquitecturas de 32 bits»,* dijo Kellas.