BOLETÍN DE ALERTA

Boletín Nro.: 2022-44
Fecha de publicación: 27/10/2022
Tema: Vulnerabilidad de ejecución de código arbitrario en SQLite.

Las versiones afectadas de SQLite son:

- SQLite, versiones de 1.0.12 a 3.39.1.

Descripción:

Se ha publicado un aviso de seguridad sobre una vulnerabilidad que afecta a aplicaciones que utilizan el sistema de gestión de base de datos *SQLite*, que permitiría a un atacante realizar ejecución de código arbitrario en el sistema afectado. La misma puede ser explotada en sistemas de 64 bits. Actualmente para esta vulnerabilidad ya existe *PoC* publicado en Internet.

La vulnerabilidad identificada como CVE-2022-35737, de severidad "alta" y con puntuación asignada de 7.5. Esta vulnerabilidad se debe a una falla de desbordamiento de enteros provocado por las funciones *printf y sqlite3_str_vappendf* de SQLite. Esto ocurre cuando se ingresan grandes cadenas de caracteres a la función *printf,* además, cuando la cadena contiene los tipos de sustitución de formato *%Q, %q o %w derivando en que el programa no responda y se cuelgue.* Así también, se ha demostrado que si la cadena contiene el carácter especial *!* para habilitar el escaneo de caracteres en unicode es posible lograr la ejecución de código arbitrario, en otros casos el programa se cuelga o ingresa en un loop. Cabe destacar que la ejecución de código arbitrario se confirma cuando la biblioteca se compila sin controles controlados de pila (*stack canaries*).

Impacto:

La explotación exitosa de esta vulnerabilidad permitiría a un atacante realizar ejecución de código y causar una denegación de servicios (*DoS*).

Solución:

Recomendamos realizar la actualización correspondiente a la versión 3.39.2 de *SQLite* provista por el proveedor en el siguiente enlace:

- https://www.sqlite.org/releaselog/3_39_2.html

Información adicional:

- https://thehackernews.com/2022/10/22-year-old-vulnerability-reported-in.html

- https://nvd.nist.gov/vuln/detail/CVE-2022-35737
- https://blog.trailofbits.com/2022/10/25/sqlite-vulnerability-july-2022-library-api/
- https://www.sqlite.org/releaselog/3_39_2.html