Alerta de seguridad cibernética	9VSA20-00226-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	26 de mayo de 2020
Última revisión	26 de mayo de 2020

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida de SQLite referente a dos vulnerabilidades que afectan al sistema de gestión de bases de datos relacionales. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidades

CVE-2020-13434
CVE-2020-13435

CVE-2020-13434

Debido a un error de desbordamiento de enteros en memoria en la función “sqlite3_str_vappendf()” en “printf.c”, un atacante remoto podría entregarle datos especialmente diseñados a la aplicación, gatillar el error en memoria y causar una denegación de servicios en el sistema afectado.

Productos Afectados

Afecta a todas las versiones de SQLite desde que la función “printf()” fue introducida en la versión 3.8.2 (03-02-2014).

Mitigación

Actualizar a la versión 3.33.0 de SQLite.

Enlaces

https://www.sqlite.org/src/info/23439ea582241138
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13434

CVE-2020-13435

Debido a la insuficiente validación de datos ingresados por el usuario en la función “sqlite3ExprCodeTarget()” en “expr.c”, un atacante remoto podría entregarle datos especialmente diseñados a la aplicación para causar una denegación de servicios en el sistema afectado.

Productos Afectados

Afecta a todas las versiones de SQLite desde la versión 3.0.

Mitigación

Actualizar a la versión 3.33.0 de SQLite.

Enlaces

https://www.sqlite.org/src/info/7a5279a25c57adf1
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13435