Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Stranger Strings: A 22-year-old vulnerability in SQLite

Date of Publication	Admiralty code	TA Number
October 26, 2022	A1	TA2022234

Summary

A vulnerability in the SQLite library API has been assigned CVE-2022-35737, which could allow an attacker to crash or control programs.

CVE Table

CVE	NAME	PATCH
CVE-2022-35737	Improper Validation of Array Index in SQLite	✓

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0008** Lateral Movement	**TA0040** Impact	**T1210** Exploitation of Remote Services
T1203 Exploitation for Client Execution	**T1489** Service Stop		

Technical Details

#1 In vulnerable systems, CVE-2022-35737 can be exploited if a large string input is passed to the SQLite implementations of the printf functions along with a format string containing %Q, %q, or %w format substitutions. This is enough to crash the program.

#2 This array-bounds overflow vulnerability cannot be exploited using SQL, nor by providing SQLite with a corrupt database file, and a few specific C-language interfaces require very long string arguments (greater than 2 billion bytes in length) to exploit it.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-35737	MySQL Workbench: 8.0.11 - 8.0.30	cpe:2.3:a:sqlite:sqlite:-:*:*:*:*:*:*:*	CWE-129

Patch Links

https://www.sqlite.org/cves.html

References

https://blog.trailofbits.com/2022/10/25/sqlite-vulnerability-july-2022-library-api/

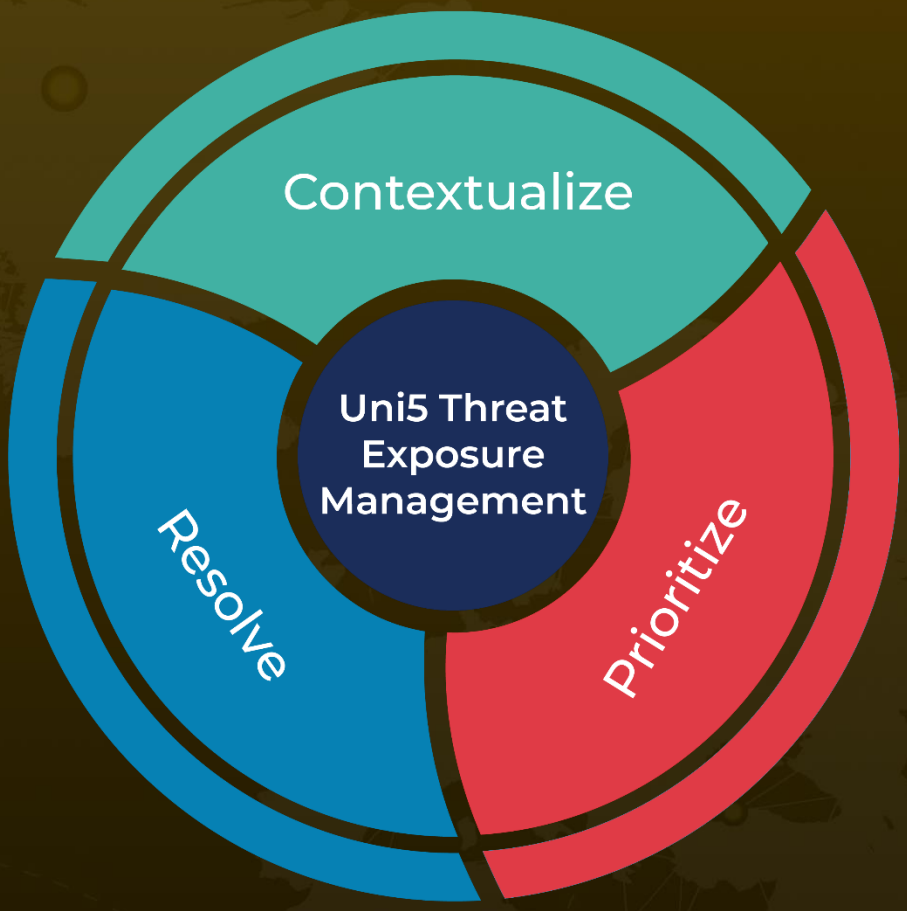
https://nvd.nist.gov/vuln/detail/CVE-2022-35737

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

What Next?

At **HivePro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

October 26, 2022 . 6:54 AM

More at www.hivepro.com