sqlite ATTACH allows some filesystem access

Moderate **directionless** published **GHSA-4g56-2482-x7q8** on Dec 14, 2020

Package

osquery

Affected versions

< 4.6.0

Patched versions

None

Description

Impact

By using sqlite's `ATTACH` verb, someone with administrative access to osquery can cause reads and writes to arbitrary sqlite databases on disk. This *does* allow arbitrary files to be created, but they will be sqlite databases.

It does not appear to allow existing non-sqlite files to be overwritten.

Create new files:

```
$ ls  /tmp/out.db; echo "ATTACH DATABASE '/tmp/out.db' AS o; CREATE TABLE o.out (a text); INSERT INTO o.out (a) VALUES('hello world');" | osqueryd -S ; ls /tmp/out.db
ls: /tmp/out.db: No such file or directory
/tmp/out.db
```

Existing non-sqlite files:

```
$ echo "ATTACH DATABASE '/tmp/existing' AS o; CREATE TABLE o.out (a text); INSERT INTO o.out (a) VALUES('hello world');" | osqueryd -S
Error: near line 1: file is not a database
```

Patches

This has been patched in osquery 4.6.0.

Workarounds

- In some deployments, the people with access to these interfaces may be considered administrators.
- In some deployments, configuration is managed by a central tool. This tool can filter for the `ATTACH` keyword
- osquery can be run as non-root user. Because this also limits the desired access levels, this requires deployment specific testing and configuration.

References

https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/SQL%20Injection/SQLite%20Injection.md#remote-command-execution-using-sqlite-command---load_extension

Severity

Moderate

CVE ID

CVE-2020-26273

Weaknesses

No CWEs

Credits

martin-langhoff