New issue

Jump to bottom

Double-free vulnerability in contrib/shpsort.c #39

Closed **eldstal** opened this issue on Dec 29, 2021 · 3 comments

eldstal commented on Dec 29, 2021 • edited Contributor

Summary

The buffer `copy` is freed twice, leading to possible memory corruption or vulnerability.

Cause

In `split()`, at shpsort.c:107, the buffer `copy` is free'd. `realloc()` fails on line 110, the buffer `copy` is freed again at shpsort.c:116.

Impact

A double-free bug can lead to an attacker gaining control over the values returned from `malloc()`, which in turn may allow both disclosure of sensitive data (e.g. bypassing additional safety features) or in the worst case hostile code execution.

Vulnerable version

- contrib/shpsort (commit `21ae8fc`)

Proposed mitigation

Remove line 116, as it is redundant.

mloskot commented on Jan 3 Member

Instead of opening the issue, a pull request could be a time saver

eldstal added a commit to eldstal/shapelib that referenced this issue on Jan 3

Remove double free() in contrib/shpsrt, issue OSGeo#39 ... c75b928

eldstal mentioned this issue on Jan 3

Remove double free() in contrib/shpsrt, issue #39 #40

Merged

eldstal commented on Jan 3 — Contributor — Author

Fair point.

rouault added a commit that referenced this issue on Jan 3

Merge pull request #40 from eldstal/issue_39 ... df1e996

rouault closed this as completed on Jan 3

---

eldstal commented on Feb 22 — Contributor — Author

This vulnerability has been assigned CVE-2022-0699 by the Red Hat CNA.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants