memory leaks in function cmdopts_parse #332

Closed xiaoxiaoafeifei opened this issue on Jul 20 · 4 comments · Fixed by #333

xiaoxiaoafeifei commented on Jul 20 • edited

Hi,
I found a memory leak bug in function cmdopts_parse on Version 3.0.6

Here's valgrind log:

```
test@9e5cd2886520:~/fuzz_target/jasper-3.0.6/builder$ valgrind --show-reachable=yes /usr/local/bin/jasper --input test1 --output /dev/null --output-format
==548691== Memcheck, a memory error detector
==548691== Copyright (C) 2002-2015, and GNU GPL'd, by Julian Seward et al.
==548691== Using Valgrind-3.11.0 and LibVEX; rerun with -h for copyright info
==548691== Command: ./src/app/jasper --force-srgb --input /home/zll/out_bk/crashes/test1 --output /dev/null --output-format
==548691==
missing argument for option --output-format
For more information on how to use this command, type:
jasper --help
==548691==
==548691== HEAP SUMMARY:
==548691== in use at exit: 8,336 bytes in 1 blocks
==548691== total heap usage: 1 allocs, 0 frees, 8,336 bytes allocated
==548691==
==548691== LEAK SUMMARY:
==548691== definitely lost: 0 bytes in 0 blocks
==548691== indirectly lost: 0 bytes in 0 blocks
==548691== possibly lost: 0 bytes in 0 blocks
==548691== still reachable: 8,336 bytes in 1 blocks
==548691== suppressed: 0 bytes in 0 blocks
```

Steps to Reproduce

1. /usr/local/bin/cmake -DJAS_ENABLE_DOC:BOOL=OFF -B builder
2. make & make install

3. valgrind --show-reachable=yes /usr/local/bin/jasper --input input_file --output /dev/null --output-format
   input_file.zip

xiaoxiaoafeifei mentioned this issue on Jul 20

fix memory leaks in function cmdopts_parse #333

Merged

jubalh commented on Jul 22 — Member

Can you upload the input file here?

xiaoxiaoafeifei commented on Jul 25 — Author

> Can you upload the input file here?

Hi, I have uploaded the input file

jubalh closed this as completed in #333 on Jul 25

jubalh commented on Jul 25 — Member

Thanks for your report and accompanying PR!

After applying your PR:

```
valgrind --show-reachable=yes ./src/app/jasper --input ~/Downloads/input_file --output /dev/null --output-format
==13710== Memcheck, a memory error detector
==13710== Copyright (C) 2002-2022, and GNU GPL'd, by Julian Seward et al.
==13710== Using Valgrind-3.19.0 and LibVEX; rerun with -h for copyright info
==13710== Command: ./src/app/jasper --input /home/michael/Downloads/input_file --output /dev/null
==13710==
==13710== HEAP SUMMARY:
==13710==     in use at exit: 0 bytes in 0 blocks
==13710==   total heap usage: 1 allocs, 1 frees, 8,336 bytes allocated
==13710==
==13710== All heap blocks were freed -- no leaks are possible
==13710==
==13710== For lists of detected and suppressed errors, rerun with: -s
==13710== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

jubalh commented on Sep 16 Member

Apparently this issue has been assigned CVE-2022-2963.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

fix memory leaks in function cmdopts_parse
xiaoxiaoafeifei/jasper

2 participants