ckolivas / lrzip Public

Code   Issues 15   Pull requests 2   Actions   Projects   Wiki   ···

New issue   Jump to bottom

UndefinedBehaviorSanitizer: invalid shifts #224

Open   **pietroborrello** opened this issue on May 4 · 0 comments

pietroborrello commented on May 4 • edited

Describe the bug

UndefinedBehaviorSanitizer: two runtime errors that expose invalid integer shifts in the library.

To Reproduce

Built lrzip using clang-10 with `CXXFLAGS` and/or `CFLAGS` `='-O1 -fsanitize=address -fsanitize=array-bounds,bool,builtin,enum,float-divide-by-zero,function,integer-divide-by-zero,null,object-size,return,returns-nonnull-attribute,shift,signed-integer-overflow,unreachable,vla-bound,vptr'`

commit: 3495188

UBSAN Output

```
$ ./lrzip -d ./id:000000,sig:06,src:000057+000060,time:234495,op:splice,rep:8,trial:0 -o asd
Output filename is: asd
lrzip.c:208:36: runtime error: left shift of 2149580800 by 32 places cannot be represented in type
'i64' (aka 'long')
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior lrzip.c:208:36 in
Invalid expected size -9214364837600034554

$ ./lrzip -d ../../fizzbench-second-bench/cve-unique/lrzip-
lrzip_decompress_fuzzer/id:000001,sig:06,src:000124+000094,time:315933,op:splice,rep:2,trial:3 -o
output
Output filename is: output
Decompressing...
libzpaq/libzpaq.cpp:804:58: runtime error: left shift of negative value -70
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior libzpaq/libzpaq.cpp:804:58 in
```

testcases:
testcases.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant