New issue

Jump to bottom

UBSAN: shift exponent is too large #1293

Open **pietroborrello** opened this issue on Feb 17 · 0 comments

Labels 1 stb_image

pietroborrello commented on Feb 17 • edited

Describe the bug

Several `UBSAN runtime error: shift exponent 32 is too large for 32-bit type 'unsigned int'` and similar

To Reproduce

Built stb according to the oss-fuzz script with `CXXFLAGS='-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'`

UBSAN Output

```
$ ./stbi_read_fuzzer ./id:000116,sig:06,src:001260,time:12860161,op:havoc,rep:16,trial:1503866
INFO: Seed: 1313754043
INFO: Loaded 1 modules   (6883 inline 8-bit counters): 6883 [0x5e1b33, 0x5e3616),
INFO: Loaded 1 PC tables (6883 PCs): 6883 [0x573228,0x58e058),
stbi_read_fuzzer: Running 1 inputs 1 time(s) each.
Running: id:000116,sig:06,src:001260,time:12860161,op:havoc,rep:16,trial:1503866
src/stb/tests/../stb_image.h:2065:27: runtime error: shift exponent 32 is too large for 32-bit
type 'unsigned int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior src/stb/tests/../stb_image.h:2065:27 in
Executed id:000116,sig:06,src:001260,time:12860161,op:havoc,rep:16,trial:1503866 in 2 ms
***
*** NOTE: fuzzing was not performed, you have only
***       executed the target code on a fixed set of inputs.
***
```

Crashing files

ubsan-shift-too-large.zip

nothings added the 1 stb_image label on Feb 17

NeilBickford-NV mentioned this issue on Feb 23

Additional stb_image fixes for bugs from ossfuzz and issues 1289, 1291, 1292, and 1293
#1297

Open

slouken pushed a commit to libsdl-org/SDL_image that referenced this issue on May 28

`stb_image.h: imported three fuzz fixes by Neil Bickford from mainstream` ... `04562ed`

Assignees

No one assigned

Labels

1 stb_image

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants