nothings / stb Public

<> Code ⊙ Issues 99 Pull requests 75 Discussions Actions Projects •••

New issue

Jump to bottom

UBSAN: integer overflow #1292

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

Labels 1 stb_image

pietroborrello commented on Feb 17 • edited

Describe the bug

`UBSAN: runtime error: signed integer overflow: -126340289 * 17 cannot be represented in type 'int'`

and

`UBSAN: runtime error: signed integer overflow: -2147450975 + -32767 cannot be represented in type 'int'`

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:000130,sig:06,src:002266+002478,time:16238914,op:splice,rep:16,trial:1492432

INFO: Seed: 1429753284
INFO: Loaded 1 modules   (6883 inline 8-bit counters): 6883 [0x5e1b33, 0x5e3616),
INFO: Loaded 1 PC tables (6883 PCs): 6883 [0x573228,0x58e058),
../cve_exp/work_LIBFUZZER_HELPER_STB_STBI_READ_FUZZER/out/stbi_read_fuzzer: Running 1 inputs 1
time(s) each.
Running: id:000130,sig:06,src:002266+002478,time:16238914,op:splice,rep:16,trial:1492432
src/stb/tests/../stb_image.h:2251:29: runtime error: signed integer overflow: -1073741919 * 2
cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior src/stb/tests/../stb_image.h:2251:29 in
src/stb/tests/../stb_image.h:2249:35: runtime error: signed integer overflow: -2147450975 + -32767
cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior src/stb/tests/../stb_image.h:2249:35 in
Executed id:000130,sig:06,src:002266+002478,time:16238914,op:splice,rep:16,trial:1492432 in 76 ms
***
*** NOTE: fuzzing was not performed, you have only
***       executed the target code on a fixed set of inputs.
***
```

Crashing files

ubsan-integer-overflow.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