New issue

Jump to bottom

UndefinedBehaviorSanitizer: signed integer overflow #3557

Closed **pietroborrello** opened this issue on Apr 29 · 0 comments

pietroborrello commented on Apr 29

Describe the bug

UndefinedBehaviorSanitizer: signed integer overflow in hb-ot-shape-fallback.cc

To Reproduce

Built harfbuzz-shape-fuzzer using clang-10 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'`

commit: `7f7ebdc`

UBSAN Output

```
$ ./hb-shape-fuzzer id:000000,sig:06,src:014111,time:17042722,op:havoc,rep:2,trial:1
INFO: Seed: 3794760496
INFO: Loaded 1 modules   (85057 inline 8-bit counters): 85057 [0x1066033, 0x107ac74),
INFO: Loaded 1 PC tables (85057 PCs): 85057 [0x107ac78,0x11c7088),
hb-shape-fuzzer: Running 1 inputs 1 time(s) each.
Running: id:000000,sig:06,src:014111,time:17042722,op:havoc,rep:2,trial:1
harfbuzz/src/hb-ot-shape-fallback.cc:262:67: runtime error: signed integer overflow: 6 -
-2147483648 cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior harfbuzz/src/hb-ot-shape-
fallback.cc:262:67 in
harfbuzz/src/hb-ot-shape-fallback.cc:279:45: runtime error: signed integer overflow: -2147483648 +
-2147483648 cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior harfbuzz/src/hb-ot-shape-
fallback.cc:279:45 in
harfbuzz/src/hb-ot-shape-fallback.cc:279:67: runtime error: signed integer overflow: 0 -
-2147483648 cannot be represented in type 'int'
SUMMARY: UndefinedBehaviorSanitizer: undefined-behavior harfbuzz/src/hb-ot-shape-
fallback.cc:279:67 in
Executed id:000000,sig:06,src:014111,time:17042722,op:havoc,rep:2,trial:1 in 4 ms
```

testcase:

harfbuzz-shape-fuzzer.zip

 **behdad** closed this as completed in `62e803b` on Jun 1

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant