marcobambini / **gravity** Public

Code Issues 26 Pull requests 4 Discussions Actions Projects ···

New issue

Jump to bottom

A Segmentation fault in gravity_ircode.c #321

Closed **seviezhou** opened this issue on Aug 30, 2020 · 1 comment

seviezhou commented on Aug 30, 2020 • edited

System info

Ubuntu x86_64, clang 6.0, gravity (latest master c79e18)

Configure

cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"

Command line

./build/gravity @@

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==75725==ERROR: AddressSanitizer: SEGV on unknown address 0x61700001045e (pc 0x000000632cf4 bp 0xfffffffffffffffc sp 0x7ffc36fe3a80 T0)
==75725==The signal is caused by a WRITE memory access.
    #0 0x632cf3 in ircode_register_pop_context_protect /home/seviezhou/gravity/src/compiler/gravity_ircode.c
    #1 0x621a1e in visit_unary_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1329:19
    #2 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #3 0x621980 in visit_unary_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1323:5
    #4 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #5 0x6185e7 in visit_compound_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:370:5
    #6 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #7 0x6185e7 in visit_compound_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:370:5
    #8 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #9 0x61dc28 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_codegen.c:994:9
    #10 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #11 0x621980 in visit_unary_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1323:5
    #12 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #13 0x621980 in visit_unary_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1323:5
    #14 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #15 0x6185e7 in visit_compound_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:370:5
    #16 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #17 0x618357 in visit_list_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:364:5
    #18 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #19 0x617b08 in gravity_codegen /home/seviezhou/gravity/src/compiler/gravity_codegen.c:2042:5
    #20 0x522249 in gravity_compiler_run /home/seviezhou/gravity/src/compiler/gravity_compiler.c:175:26
    #21 0x51e766 in main /home/seviezhou/gravity/src/cli/gravity.c:456:19
    #22 0x7f2c9afa383f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #23 0x4217a8 in _start (/home/seviezhou/gravity/build/gravity+0x4217a8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/gravity/src/compiler/gravity_ircode.c in ircode_register_pop_context_protect
==75725==ABORTING
```

POC

SEGV-ircode_register_pop_context_protect-gravity_ircode.zip

seviezhou changed the title ~~A Segmentation fault in gravity_codegen.c:1329:19~~ A Segmentation fault in gravity_ircode.c on Aug 30, 2020

marcobambini commented on Aug 31, 2020 Owner

Thanks a lot for your feedback.
Fixed by `115ee00`

marcobambini closed this as completed on Aug 31, 2020

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants