

New issue

Jump to bottom

A Segmentation fault in gravity_ircode.c:428:20 #315

Closed seviezhou opened this issue on Aug 7, 2020 · 1 comment

seviezhou commented on Aug 7, 2020

System info

Ubuntu x86_64, clang 6.0, gravity (latest master [ecbee9f](#))

Configure

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

Command line

./build/gravity -o /tmp/grav -q -c @@

Output

Segmentation fault

AddressSanitizer output

```
AddressSanitizer:DEADLYSIGNAL
=====
==37643==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000006321dd bp 0x617000000400 sp 0x7fff9ce94610 T0)
==37643==The signal is caused by a READ memory access.
==37643==Hint: address points to the zero page.
#0 0x6321dd in ircode_add_check /home/seviezhou/gravity/src/compiler/gravity_ircode.c:428:20
#1 0x6213cd in visit_binary_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1281:9
#2 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#3 0x61dc28 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_codegen.c:994:9
#4 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#5 0x626eca in visit_postfix_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1571:13
#6 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#7 0x618357 in visit_list_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:364:5
#8 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#9 0x617b08 in gravity_codegen /home/seviezhou/gravity/src/compiler/gravity_codegen.c:2042:5
#10 0x522249 in gravity_compiler_run /home/seviezhou/gravity/src/compiler/gravity_compiler.c:175:26
#11 0x51e766 in main /home/seviezhou/gravity/src/cli/gravity.c:456:19
#12 0x7f4cbb2b83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#13 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:428:20 in ircode_add_check
==37643==ABORTING
```


POC

[SEGV-ircode_add_check-gravity_ircode-428.zip](#)

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

