

New issue

Jump to bottom

# A Segmentation fault in gravity\_value.c:2382:44 #314

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
=====
==77246==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f62c70ba7c6 bp 0x7ffd17a4f500 sp 0x7ffd17a4ec88 T0)
==77246==The signal is caused by a READ memory access.
==77246==Hint: address points to the zero page.
#0 0x7f62c70ba7c5 in strlen /build/glibc-e6zv40/glibc-2.23/string/../sysdeps/x86_64/strlen.S:76
#1 0x481f8c in __interceptor_strlen.part.32 /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:341
#2 0x5d3d89 in gravity_string_to_value /home/seviezhou/gravity/src/shared/gravity_value.c:2382:44
#3 0x61ceca in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_codegen.c:966:32
#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 0x61dc28 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_codegen.c:994:9
#8 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#9 0x626eca in visit_postfix_expr /home/seviezhou/gravity/src/compiler/gravity_codegen.c:1571:13
#10 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#11 0x618357 in visit_list_stmt /home/seviezhou/gravity/src/compiler/gravity_codegen.c:364:5
#12 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
#13 0x617b08 in gravity_codegen /home/seviezhou/gravity/src/compiler/gravity_codegen.c:2042:5
#14 0x522249 in gravity_compiler_run /home/seviezhou/gravity/src/compiler/gravity_compiler.c:175:26
#15 0x51e766 in main /home/seviezhou/gravity/src/cli/gravity.c:456:19
#16 0x7f62c704f83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#17 0x4217a8 in _start (/home/seviezhou/gravity/build/gravity+0x4217a8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-e6zv40/glibc-2.23/string/../sysdeps/x86_64/strlen.S:76 in strlen
==77246==ABORTING
```


## POC

[SEGV-gravity\\_string\\_to\\_value-gravity\\_value-2382.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

