New issue

Jump to bottom

A Segmentation fault in gravity_core.c:1100:5 #319

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

seviezhou commented on Aug 30, 2020

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
=================================================================
==22249==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (pc 0x0000005760de bp 0x7fffd48f3730 sp 0x7fffd48f34b0 T0)
==22249==The signal is caused by a READ memory access.
==22249==Hint: address points to the zero page.
    #0 0x5760dd in list_iterator_next /home/seviezhou/gravity/src/runtime/gravity_core.c:1100:5
    #1 0x5a4053 in gravity_vm_exec /home/seviezhou/gravity/src/runtime/gravity_vm.c:1236:39
    #2 0x5c4ec1 in gravity_vm_loadclosure /home/seviezhou/gravity/src/runtime/gravity_vm.c:1655:5
    #3 0x5c4ec1 in gravity_vm_runmain /home/seviezhou/gravity/src/runtime/gravity_vm.c:1784
    #4 0x51e8ef in main /home/seviezhou/gravity/src/cli/gravity.c:481:9
    #5 0x7fcdc0ec883f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #6 0x4217a8 in _start (/home/seviezhou/gravity/build/gravity+0x4217a8)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/seviezhou/gravity/src/runtime/gravity_core.c:1100:5 in list_iterator_next
==22249==ABORTING
```

POC

SEGV-list_iterator_next-gravity_core-1100.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