New issue

Jump to bottom

A heap-buffer-overflow in gravity_ast.c:90:41 can cause abort #313

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

seviezhou commented on Aug 7, 2020 • edited

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

```
WARNING ERROR on 0 (1,1): Unknown macro token. Declaration will be ignored.
SEMANTIC ERROR on 0 (1,39): Identifier resudb not found.
*** Error in `./build/gravity': free(): invalid next size (fast): 0x0000000001b32470 ***
======= Backtrace: =========
/lib/x86_64-linux-gnu/libc.so.6(+0x777f5)[0x7f17e014d7f5]
/lib/x86_64-linux-gnu/libc.so.6(+0x8038a)[0x7f17e015638a]
/lib/x86_64-linux-gnu/libc.so.6(cfree+0x4c)[0x7f17e015a58c]
./build/gravity[0x4602a0]
./build/gravity(gvisit+0x1c6)[0x41c8a2]
./build/gravity[0x45fed0]
./build/gravity[0x4601da]
./build/gravity(gvisit+0x222)[0x41c8fe]
./build/gravity[0x45fb58]
./build/gravity(gvisit+0xb2)[0x41c78e]
./build/gravity[0x460038]
./build/gravity(gvisit+0x1f4)[0x41c8d0]
./build/gravity[0x4605be]
./build/gravity(gvisit+0x2be)[0x41c99a]
./build/gravity[0x45fa35]
./build/gravity(gvisit+0x84)[0x41c760]
./build/gravity(gnode_free+0x103)[0x460e31]
./build/gravity[0x40926e]
./build/gravity(gravity_compiler_run+0x223)[0x4096ae]
./build/gravity(main+0x26b)[0x408c43]
/lib/x86_64-linux-gnu/libc.so.6(__libc_start_main+0xf0)[0x7f17e00f6840]
./build/gravity(_start+0x29)[0x407af9]
======= Memory map: ========
00400000-0047d000 r-xp 00000000 08:11 4598269                            /home/seviezhou/gravity/build/gravity
0067c000-0067d000 r--p 0007c000 08:11 4598269                            /home/seviezhou/gravity/build/gravity
0067d000-0067e000 rw-p 0007d000 08:11 4598269                            /home/seviezhou/gravity/build/gravity
0067e000-0067f000 rw-p 00000000 00:00 0
01b10000-01b52000 rw-p 00000000 00:00 0                                  [heap]
7f17dbde8000-7f17dbdff000 r-xp 00000000 08:02 12582916                   /lib/x86_64-linux-gnu/libgcc_s.so.1
7f17dbdff000-7f17dbffe000 ---p 00017000 08:02 12582916                   /lib/x86_64-linux-gnu/libgcc_s.so.1
7f17dbffe000-7f17dbfff000 r--p 00016000 08:02 12582916                   /lib/x86_64-linux-gnu/libgcc_s.so.1
7f17dbfff000-7f17dc000000 rw-p 00017000 08:02 12582916                   /lib/x86_64-linux-gnu/libgcc_s.so.1
7f17dc000000-7f17dc021000 rw-p 00000000 00:00 0
7f17dc021000-7f17e0000000 ---p 00000000 00:00 0
7f17e00d6000-7f17e0296000 r-xp 00000000 08:02 12582935                   /lib/x86_64-linux-gnu/libc-2.23.so
7f17e0296000-7f17e0496000 ---p 001c0000 08:02 12582935                   /lib/x86_64-linux-gnu/libc-2.23.so
7f17e0496000-7f17e049a000 r--p 001c0000 08:02 12582935                   /lib/x86_64-linux-gnu/libc-2.23.so
7f17e049a000-7f17e049c000 rw-p 001c4000 08:02 12582935                   /lib/x86_64-linux-gnu/libc-2.23.so
7f17e049c000-7f17e04a0000 rw-p 00000000 00:00 0
7f17e04a0000-7f17e05a8000 r-xp 00000000 08:02 12582941                   /lib/x86_64-linux-gnu/libm-2.23.so
7f17e05a8000-7f17e07a7000 ---p 00108000 08:02 12582941                   /lib/x86_64-linux-gnu/libm-2.23.so
7f17e07a7000-7f17e07a8000 r--p 00107000 08:02 12582941                   /lib/x86_64-linux-gnu/libm-2.23.so
7f17e07a8000-7f17e07a9000 rw-p 00108000 08:02 12582941                   /lib/x86_64-linux-gnu/libm-2.23.so
7f17e07a9000-7f17e07cf000 r-xp 00000000 08:02 12582973                   /lib/x86_64-linux-gnu/ld-2.23.so
7f17e099d000-7f17e09a1000 rw-p 00000000 00:00 0
7f17e09cd000-7f17e09ce000 rw-p 00000000 00:00 0
7f17e09ce000-7f17e09cf000 r--p 00025000 08:02 12582973                   /lib/x86_64-linux-gnu/ld-2.23.so
7f17e09cf000-7f17e09d0000 rw-p 00026000 08:02 12582973                   /lib/x86_64-linux-gnu/ld-2.23.so
7f17e09d0000-7f17e09d1000 rw-p 00000000 00:00 0
7ffd38896000-7ffd388b7000 rw-p 00000000 00:00 0                          [stack]
7ffd3899f000-7ffd389a1000 r--p 00000000 00:00 0                          [vvar]
7ffd389a1000-7ffd389a3000 r-xp 00000000 00:00 0                          [vdso]
ffffffffff600000-ffffffffff601000 r-xp 00000000 00:00 0                  [vsyscall]
Aborted
seviezhou@ubun
```

AddressSanitizer output

```
=================================================================
==76343==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b00000041c at pc 0x00000060c196 bp 0x7fffdcef1f40 sp 0x7fffdcef1f38
READ of size 2 at 0x60b00000041c thread T0
    #0 0x60c195 in gnode_function_add_upvalue /home/seviezhou/gravity/src/compiler/gravity_ast.c:90:41
    #1 0x55cef2 in lookup_identifier /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:239:21
    #2 0x557feb in visit_identifier_expr /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:1156:23
    #3 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #4 0x5520a8 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:750:17
    #5 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #6 0x552bb6 in visit_variable_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:793:22
    #7 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #8 0x54e2e7 in visit_compound_stmt /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:565:5
    #9 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #10 0x5520a8 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:750:17
    #11 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #12 0x552bb6 in visit_variable_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:793:22
    #13 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #14 0x5520a8 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:750:17
    #15 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #16 0x556481 in visit_binary_expr /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:957:5
    #17 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #18 0x5520a8 in visit_function_decl /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:750:17
    #19 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #20 0x556481 in visit_binary_expr /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:957:5
    #21 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #22 0x54dcf7 in visit_list_stmt /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:553:5
    #23 0x563b63 in gvisit /home/seviezhou/gravity/src/compiler/gravity_visitor.c
    #24 0x54d6a5 in gravity_semacheck2 /home/seviezhou/gravity/src/compiler/gravity_semacheck2.c:1237:5
    #25 0x5221d6 in gravity_compiler_run /home/seviezhou/gravity/src/compiler/gravity_compiler.c:171:15
    #26 0x51e766 in main /home/seviezhou/gravity/src/cli/gravity.c:456:19
    #27 0x7f6e049cd83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #28 0x4217a8 in _start (/home/seviezhou/gravity/build/gravity+0x4217a8)

0x60b00000041c is located 4 bytes to the right of 104-byte region [0x60b0000003b0,0x60b000000418)
allocated by thread T0 here:
    #0 0x4e5bd0 in calloc /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:97
    #1 0x5d0f41 in gravity_calloc /home/seviezhou/gravity/src/shared/gravity_memory.c:19:12
    #2 0x53fe30 in parse_enum_declaration /home/seviezhou/gravity/src/compiler/gravity_parser.c:1443:52
    #3 0x53fe30 in parse_declaration_statement /home/seviezhou/gravity/src/compiler/gravity_parser.c:2362
    #4 0x53d474 in parse_statement /home/seviezhou/gravity/src/compiler/gravity_parser.c:2504:59
    #5 0x53ba6c in parse_compound_statement /home/seviezhou/gravity/src/compiler/gravity_parser.c:2309:25
    #6 0x539c11 in parse_function /home/seviezhou/gravity/src/compiler/gravity_parser.c:300:63
    #7 0x53669f in parse_precedence /home/seviezhou/gravity/src/compiler/gravity_parser.c:1059:32
    #8 0x534617 in parse_infix /home/seviezhou/gravity/src/compiler/gravity_parser.c:1114:22
    #9 0x5368ec in parse_precedence /home/seviezhou/gravity/src/compiler/gravity_parser.c:1080:16
    #10 0x53dec2 in parse_expression /home/seviezhou/gravity/src/compiler/gravity_parser.c:1092:12
    #11 0x53dec2 in parse_expression_statement /home/seviezhou/gravity/src/compiler/gravity_parser.c:2477
    #12 0x53dec2 in parse_statement /home/seviezhou/gravity/src/compiler/gravity_parser.c:2510
    #13 0x52cfbf in parser_run /home/seviezhou/gravity/src/compiler/gravity_parser.c:2575:29
    #14 0x52cfbf in gravity_parser_run /home/seviezhou/gravity/src/compiler/gravity_parser.c:2658
    #15 0x5220e9 in gravity_compiler_run /home/seviezhou/gravity/src/compiler/gravity_compiler.c:161:21

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/gravity/src/compiler/gravity_ast.c:90:41 in gnode_function_add_upvalue
Shadow bytes around the buggy address:
  0x0c167fff8030: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c167fff8040: 00 00 fa fa fa fa fa fa fa fa 00 00 00 00 00 00
  0x0c167fff8050: 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa
  0x0c167fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x0c167fff8070: fa fa fa fa fa fa 00 00 00 00 00 00 00 00 00 00
=>0x0c167fff8080: 00 00 00[fa]fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c167fff8090: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c167fff80a0: fa fa 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c167fff80b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c167fff80c0: 00 00 00 00 00 00 fa fa fa fa fa fa fa fa fa fa
  0x0c167fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==76343==ABORTING
```

POC

heap-overflow-gnode_function_add_upvalue-gravity_ast-90.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