New issue

Jump to bottom

Aborted in CWriter::Write at wasm2c #1985

Closed Q1IQ opened this issue on Sep 5 · 1 comment · Fixed by #1887

Q1IQ commented on Sep 5

Environment

```
OS      : Linux ubuntu 5.15.0-46-generic #49~20.04.1-Ubuntu SMP Thu Aug 4 19:15:44 UTC 2022 x86_64
x86_64 x86_64 GNU/Linux
Commit  : 3054d61f703d609995798f872fc86b462617c294
Version : 1.0.29
Build   : make clang-debug-asan
```

Proof of concept

poc_wasm2c-1.wasm
poc_wasm2c-1.wasm.zip

Stack dump

```
gdb /wabt/out/clang/Debug/asan/wasm2c
pwndbg> r  --enable-multi-memory ./poc_wasm2c-1.wasm
context:
LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA
─────────────────────────────────[ REGISTERS ]─────────────────────────────────
 RAX  0x0
*RBX  0x7ffff7a357c0 ◂— 0x7ffff7a357c0
*RCX  0x7ffff7a7b00b (raise+203) —▸ 0x10824848b48 ◂— 0x0
 RDX  0x0
*RDI  0x2
*RSI  0x7fffffff6990 ◂— 0x0
 R8   0x0
*R9   0x7fffffff6990 ◂— 0x0
*R10  0x8
*R11  0x246
*R12  0x43e420 (_start) ◂— endbr64
*R13  0x7fffffffe070 ◂— 0x3
```

```
 R14  0x0
 R15  0x0
*RBP  0x7fffffff88f0 —▸ 0x7fffffff8930 —▸ 0x7fffffffa650 —▸ 0x7fffffffa690 —▸ 0x7fffffffc3c0 ◂—
...
*RSP  0x7fffffff6990 ◂— 0x0
*RIP  0x7ffff7a7b00b (raise+203) —▸ 0x10824848b48 ◂— 0x0
───────────────────────────────────[ DISASM ]───────────────────────────────────
 ► 0x7ffff7a7b00b <raise+203>    mov    rax, qword ptr [rsp + 0x108]
   0x7ffff7a7b013 <raise+211>    xor    rax, qword ptr fs:[0x28]
   0x7ffff7a7b01c <raise+220>    jne    raise+260                <raise+260>
    ↓
   0x7ffff7a7b044 <raise+260>    call   __stack_chk_fail                <__stack_chk_fail>

   0x7ffff7a7b049                nop    dword ptr [rax]
   0x7ffff7a7b050 <killpg>       endbr64
   0x7ffff7a7b054 <killpg+4>     test   edi, edi
   0x7ffff7a7b056 <killpg+6>     js     killpg+16                <killpg+16>

   0x7ffff7a7b058 <killpg+8>     neg    edi
   0x7ffff7a7b05a <killpg+10>    jmp    kill                <kill>

   0x7ffff7a7b05f <killpg+15>    nop
───────────────────────────────────[ STACK ]────────────────────────────────────
00:0000│ rsi r9 rsp 0x7fffffff6990 ◂— 0x0
01:0008│            0x7fffffff6998 ◂— '(ut)(x))unimplemented: %'
02:0010│            0x7fffffff69a0 ◂— 'unimplemented: %'
03:0018│            0x7fffffff69a8 ◂— 'ented: %'
04:0020│            0x7fffffff69b0 ◂— 0x0
... ↓               3 skipped
─────────────────────────────────[ BACKTRACE ]──────────────────────────────────
 ► f 0   0x7ffff7a7b00b raise+203
   f 1   0x7ffff7a5a859 abort+299
   f 2         0x52769e
   f 3         0x5315c3
   f 4         0x52760d
   f 5         0x5315c3
   f 6         0x52760d
   f 7         0x51dd51
────────────────────────────────────────────────────────────────────────────────


backtrace_msg:
#0  __GI_raise (sig=sig@entry=6) at ../sysdeps/unix/sysv/linux/raise.c:50
#1  0x00007ffff7a5a859 in __GI_abort () at abort.c:79
#2  0x000000000052769e in wabt::(anonymous namespace)::CWriter::Write (this=0x7fffffffce30,
exprs=...) at ../../../../src/c-writer.cc:1969
#3  0x00000000005315c3 in wabt::(anonymous namespace)::CWriter::Write<wabt::(anonymous
namespace)::Newline, wabt::intrusive_list<wabt::Expr> const&> (this=0x7fffffffce30, t=..., u=...)
at ../../../../src/c-writer.cc:205
#4  0x000000000052760d in wabt::(anonymous namespace)::CWriter::Write (this=0x7fffffffce30,
exprs=...) at ../../../../src/c-writer.cc:1945
#5  0x00000000005315c3 in wabt::(anonymous namespace)::CWriter::Write<wabt::(anonymous
namespace)::Newline, wabt::intrusive_list<wabt::Expr> const&> (this=0x7fffffffce30, t=..., u=...)
at ../../../../src/c-writer.cc:205
#6  0x000000000052760d in wabt::(anonymous namespace)::CWriter::Write (this=0x7fffffffce30,
exprs=...) at ../../../../src/c-writer.cc:1945
#7  0x000000000051dd51 in wabt::(anonymous
namespace)::CWriter::Write<wabt::intrusive_list<wabt::Expr> const&, wabt::(anonymous
namespace)::LabelDecl> (this=0x7fffffffce30, t=..., u=...) at ../../../../src/c-writer.cc:204
#8  0x000000000051bd15 in wabt::(anonymous namespace)::CWriter::Write (this=0x7fffffffce30,
func=...) at ../../../../src/c-writer.cc:1423
#9  0x000000000051b647 in wabt::(anonymous namespace)::CWriter::Write<wabt::(anonymous
namespace)::Newline, wabt::Func const&, wabt::(anonymous namespace)::Newline>
(this=0x7fffffffce30, t=..., u=..., args=...) at ../../../../src/c-writer.cc:205
#10 0x000000000051182d in wabt::(anonymous namespace)::CWriter::WriteFuncs (this=0x7fffffffce30)
at ../../../../src/c-writer.cc:1393
#11 0x0000000000500bf4 in wabt::(anonymous namespace)::CWriter::WriteCSource (this=0x7fffffffce30)
at ../../../../src/c-writer.cc:2794
#12 0x00000000004ffcd7 in wabt::(anonymous namespace)::CWriter::WriteModule (this=0x7fffffffce30,
module=...) at ../../../../src/c-writer.cc:2807
#13 0x00000000004ff48d in wabt::WriteC (c_stream=0x7fffffffdaa0, h_stream=0x7fffffffdaa0,
header_name=0x7ccce0 <str> "wasm.h", module=0x7fffffffd2b0, options=...) at ../../../../src/c-
writer.cc:2819
#14 0x00000000004f11b4 in ProgramMain (argc=3, argv=0x7fffffffe078) at
../../../../src/tools/wasm2c.cc:179
#15 0x00000000004f37f2 in main (argc=3, argv=0x7fffffffe078) at
../../../../src/tools/wasm2c.cc:190
#16 0x00007ffff7a5c083 in __libc_start_main (main=0x4f37d0 <main(int, char**)>, argc=3,
argv=0x7fffffffe078, init=<optimized out>, fini=<optimized out>, rtld_fini=<optimized out>,
stack_end=0x7fffffffe068) at ../csu/libc-start.c:308
#17 0x000000000043e44e in _start ()
```

keithw commented on Sep 17 Collaborator

This appears to be accurately (but clumsily) printing "unimplemented" because reference types are unimplemented in the current wasm2c (but wasm2c uses the default validator settings). Will be fixed by #1887 .

keithw mentioned this issue on Sep 17

wasm2c: implement the reference-types proposal #1887

Merged

keithw closed this as completed in #1887 on Oct 3

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

wasm2c: implement the reference-types proposal
fix-project/wabt

2 participants