

[New issue](#)[Jump to bottom](#)

SEGV wasm3/source/m3_exec.h:1078 in op_Select_i32_srs #379

✓ Closed

ioo0s opened this issue on Aug 28 · 2 comments

Labels

wasm-validation

ioo0s commented on Aug 28

Gdb info

Program received signal SIGSEGV, Segmentation fault.

```
0x000055555555bbf69 in op_Select_i32_srs (_pc=0x62d0000004c0, _sp=0x631000000800,
_mem=0x631000014800, _r0=3840, _fp0=1) at /home/ios/CVE/wasm3/source/m3_exec.h:1078
```

```
1078      d_m3Select_i (i32, _r0)
```

LEGEND: STACK | HEAP | CODE | DATA | RWX | RODATA

[REGISTERS

]

```
RAX 0x6311556fa980 ← 0x0
```

```
RBX 0x7fffffffefa0 ← 0x41b58ab3
```

```
RCX 0x6311556fa980 ← 0x0
```

```
RDX 0x0
```

```
RDI 0x3
```

```
RSI 0x631000000800 ← 0x100000000000
```

```
R8 0x5555555bbe20 (op_Select_i32_srs) ← endbr64
```

```
R9 0x3
```

```
R10 0x555555666940 ← 0x74726174735f /* '_start' */
```

```
R11 0x0
```

```
R12 0xffffffff9f4 ← 0x0
```

```
R13 0x7fffffffefa0 ← 0x41b58ab3
```

```
R14 0x7fffffffed340 ← 0x41b58ab3
```

```
R15 0x0
```

```
RBP 0x7fffffffcea0 → 0x7fffffffcef0 → 0x7fffffffcf40 → 0x7fffffffdd020 → 0x7fffffffdd100 ←
```

...

```
RSP 0x7fffffffce60 → 0xffffffffcf20 ← 0x0
```

```
RIP 0x5555555bbf69 (op_Select_i32_srs+329) ← mov     eax, dword ptr [rcx]
```

[DISASM

]

```
▶ 0x5555555bbf69 <op_Select_i32_srs+329>    mov     eax, dword ptr [rcx]
```

```
0x5555555bbf6b <op_Select_i32_srs+331>    mov     dword ptr [rbp - 4], eax
```

```

0x5555555bbf6e <op_Select_i32_srs+334>    cmp    dword ptr [rbp - 0xc], 0
0x5555555bbf72 <op_Select_i32_srs+338>    je     op_Select_i32_srs+347
<op_Select_i32_srs+347>

0x5555555bbf74 <op_Select_i32_srs+340>    mov    eax, dword ptr [rbp - 4]
0x5555555bbf77 <op_Select_i32_srs+343>    cdqe
0x5555555bbf79 <op_Select_i32_srs+345>    jmp    op_Select_i32_srs+352
<op_Select_i32_srs+352>
↓
0x5555555bbf80 <op_Select_i32_srs+352>    mov    qword ptr [rbp - 0x30], rax
0x5555555bbf84 <op_Select_i32_srs+356>    mov    rax, qword ptr [rbp - 0x18]
0x5555555bbf88 <op_Select_i32_srs+360>    mov    rdx, rax
0x5555555bbf8b <op_Select_i32_srs+363>    shr    rdx, 3

```

[SOURCE (CODE)

```

]-----
In file: /home/ios/CVE/wasm3/source/m3_exec.h
1073                                     \
1074     nextOp ();                       \
1075 }
1076
1077
▶ 1078 d_m3Select_i (i32, _r0)
1079 d_m3Select_i (i64, _r0)
1080
1081
1082 #define d_m3Select_f(TYPE, REG, LABEL, SELECTOR) \
1083 d_m3Op (Select_##TYPE##_##LABEL##ss)           \

```

[STACK

```

]-----
00:0000| rsp 0x7fffffffce60 → 0xaffffcf20 ← 0x0
01:0008|    0x7fffffffce68 ← 0x3ff0000000000000
02:0010|    0x7fffffffce70 ← 0xf00
03:0018|    0x7fffffffce78 → 0x631000014800 → 0x62600000100 ← 0x62600000100
04:0020|    0x7fffffffce80 → 0x631000000800 ← 0x10000000000000
05:0028|    0x7fffffffce88 → 0x62d0000004c0 → 0x5555555bdea0 (op_Return) ← endbr64
06:0030|    0x7fffffffce90 → 0x141b58ab3 ← 0x0
07:0038|    0x7fffffffce98 ← 0x55550000f00

```

[BACKTRACE

```

]-----
▶ f 0  0x5555555bbf69 op_Select_i32_srs+329
f 1  0x5555555a8fc5 op_f64_Ceil_s+261
f 2  0x5555555a55e6 op_i32_Divide_rs+422
f 3  0x5555555bf506 op_f32_Load_f32_s+838
f 4  0x5555555caca2 op_i32_Store_i32_ss+994
f 5  0x5555555ba807 op_SetSlot_i32+263
f 6  0x5555555b939e op_MemGrow+350
f 7  0x5555555aa330 op_i32_EqualToZero_s+272

```

Asan Info

AddressSanitizer:DEADLYSIGNAL

=====

==3977==ERROR: AddressSanitizer: SEGV on unknown address 0x63108b682980 (pc 0x55c322d9df69 bp 0x7ffc71ba1260 sp 0x7ffc71ba1220 T0)

==3977==The signal is caused by a READ memory access.

```
#0 0x55c322d9df68 in op_Select_i32_srs /home/ios/CVE/wasm3/source/m3_exec.h:1078
#1 0x55c322d8afc4 in op_f64_Ceil_s /home/ios/CVE/wasm3/source/m3_exec.h:272
#2 0x55c322d875e5 in op_i32_Divide_rs /home/ios/CVE/wasm3/source/m3_exec.h:231
#3 0x55c322da1505 in op_f32_Load_f32_s /home/ios/CVE/wasm3/source/m3_exec.h:1341
#4 0x55c322dacca1 in op_i32_Store_i32_ss /home/ios/CVE/wasm3/source/m3_exec.h:1449
#5 0x55c322d9c806 in op_SetSlot_i32 /home/ios/CVE/wasm3/source/m3_exec.h:941
#6 0x55c322d9b39d in op_MemGrow /home/ios/CVE/wasm3/source/m3_exec.h:704
#7 0x55c322d8c32f in op_i32_EqualToZero_s /home/ios/CVE/wasm3/source/m3_exec.h:282
#8 0x55c322d9bf1b in op_Entry /home/ios/CVE/wasm3/source/m3_exec.h:808
#9 0x55c322dc168a in RunCode /home/ios/CVE/wasm3/source/m3_exec_defs.h:58
#10 0x55c322dc76cc in m3_CallArgv /home/ios/CVE/wasm3/source/m3_env.c:953
#11 0x55c322d65510 in repl_call /home/ios/CVE/wasm3/platforms/app/main.c:274
#12 0x55c322d682f4 in main /home/ios/CVE/wasm3/platforms/app/main.c:634
#13 0x7fcbd3bff082 in __libc_start_main ../csu/libc-start.c:308
#14 0x55c322d6422d in _start (/home/ios/CVE/wasm3/build/wasm3+0x2e22d)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/ios/CVE/wasm3/source/m3_exec.h:1078 in op_Select_i32_srs

==3977==ABORTING

current commit : 7890a2097569fde845881e0b352d813573e371f9

Poc

[op_Select_i32_srs.wasm.gz](#)

ioo0s commented on Aug 28

Author

Add another poc.

current commit : 7890a2097569fde845881e0b352d813573e371f9

Asan info

AddressSanitizer:DEADLYSIGNAL

=====

==5877==ERROR: AddressSanitizer: SEGV on unknown address 0x6310731b5900 (pc 0x55571cc5f122 bp 0x7fffc6418010 sp 0x7fffc6417fd0 T0)

==5877==The signal is caused by a READ memory access.

```
#0 0x55571cc5f121 in op_Select_i32_ssr /home/ios/CVE/wasm3/source/m3_exec.h:1078
#1 0x55571cc414bc in op_f32_GreaterThanOrEqual_rs /home/ios/CVE/wasm3/source/m3_exec.h:193
#2 0x55571cc67f00 in op_i64_Load_i32_s /home/ios/CVE/wasm3/source/m3_exec.h:1355
#3 0x55571cc59a62 in op_i32_Reinterpret_f32_s_r /home/ios/CVE/wasm3/source/m3_exec.h:489
#4 0x55571cc59882 in op_i32_Reinterpret_f32_r_s /home/ios/CVE/wasm3/source/m3_exec.h:489
#5 0x55571cc59a62 in op_i32_Reinterpret_f32_s_r /home/ios/CVE/wasm3/source/m3_exec.h:489
#6 0x55571cc4ec0d in op_i32_Trunc_f32_r_s /home/ios/CVE/wasm3/source/m3_exec.h:370
#7 0x55571cc5b21e in op_f64_Reinterpret_i64_s_s /home/ios/CVE/wasm3/source/m3_exec.h:492
#8 0x55571cc4bc43 in op_f64_Abs_s /home/ios/CVE/wasm3/source/m3_exec.h:271
#9 0x55571cc59a62 in op_i32_Reinterpret_f32_s_r /home/ios/CVE/wasm3/source/m3_exec.h:489
#10 0x55571cc59882 in op_i32_Reinterpret_f32_r_s /home/ios/CVE/wasm3/source/m3_exec.h:489
#11 0x55571cc5cf1b in op_Entry /home/ios/CVE/wasm3/source/m3_exec.h:808
```



```
#12 0x55571cc8268a in RunCode /home/ios/CVE/wasm3/source/m3_exec_defs.h:58
#13 0x55571cc886cc in m3_CallArgv /home/ios/CVE/wasm3/source/m3_env.c:953
#14 0x55571cc26510 in repl_call /home/ios/CVE/wasm3/platforms/app/main.c:274
#15 0x55571cc292f4 in main /home/ios/CVE/wasm3/platforms/app/main.c:634
#16 0x7f0541953082 in __libc_start_main ../csu/libc-start.c:308
#17 0x55571cc2522d in _start (/home/ios/CVE/wasm3/build/wasm3+0x2e22d)
```

AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV /home/ios/CVE/wasm3/source/m3_exec.h:1078 in op_Select_i32_ssr
==5877==ABORTING

POC

[op_Select_i32_ssr.zip](#)

  **vshymanskyy** added the **wasm-validation** label on Aug 29

 **vshymanskyy** closed this as completed on Aug 29

vshymanskyy commented on Aug 29

Member

@ioo0s sorry I will be closing any fuzzer reports, as this is covered by [#344](#)

Assignees

No one assigned

Labels

wasm-validation

Milestone

No milestone

Development

No branches or pull requests

2 participants

