wasm3 / wasm3 Public

<> Code ⊙ Issues 33 Pull requests 8 ▷ Actions Security Insights

New issue Jump to bottom

[security] Heap Overflow in NewCodePage m3_code.c:25:29 #320

Closed **zu1k** opened this issue on Apr 7 · 2 comments

zu1k commented on Apr 7 • edited

I found a heap overflow vulnerability.

Wasm3 0.5.0 has an out-of-bounds write in NewCodePage (called from Compile_BranchTable).

Recommended Security Severity: High

Poc: poc.zip

```
$ ./wasm3 --func fib poc.wasm
Error: invalid block depth
free(): corrupted unsorted chunks
zsh: IOT instruction (core dumped)  ./wasm3 --func fib poc.wasm
```

Sanitizer: address (ASAN)

```
$ ./wasm3 --func fib poc.wasm
=================================================================
==43773==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000080 at pc
0x55de9111d3b8 bp 0x7ffc6f691a90 sp 0x7ffc6f691a88
WRITE of size 4 at 0x602000000080 thread T0
    #0 0x55de9111d3b7 in NewCodePage /disk/wasm3/source/m3_code.c:25:29
    #1 0x55de9110f4c2 in AcquireCodePageWithCapacity /disk/wasm3/source/m3_env.c:1058:20
    #2 0x55de910fff78 in EnsureCodePageNumLines /disk/wasm3/source/m3_compile.c:34:28
    #3 0x55de910b2d8e in Compile_BranchTable /disk/wasm3/source/m3_compile.c:1546:1
    #4 0x55de910f6b8c in CompileBlockStatements /disk/wasm3/source/m3_compile.c:2608:1
    #5 0x55de910face1 in CompileFunction /disk/wasm3/source/m3_compile.c:2899:1
    #6 0x55de9110b1f2 in m3_FindFunction /disk/wasm3/source/m3_env.c:729:1
    #7 0x55de91096f8c in repl_call /disk/wasm3/platforms/app/main.c:256:23
    #8 0x55de91099be0 in main /disk/wasm3/platforms/app/main.c:636:26
    #9 0x7fb47abc730f in __libc_start_call_main libc-start.c
    #10 0x7fb47abc73c0 in __libc_start_main@GLIBC_2.2.5 (/usr/lib/libc.so.6+0x2d3c0)
    #11 0x55de90fb1a24 in _start (/disk/wasm3/build/wasm3+0x52a24)
```

```
0x602000000080 is located 15 bytes to the right of 1-byte region [0x602000000070,0x602000000071)
allocated by thread T0 here:
    #0 0x55de9105c869 in __interceptor_calloc (/disk/wasm3/build/wasm3+0xfd869)
    #1 0x55de911037a9 in m3_Malloc_Impl /disk/wasm3/source/m3_core.c:129:12
    #2 0x55de9111d316 in NewCodePage /disk/wasm3/source/m3_code.c:21:25
    #3 0x55de9110f4c2 in AcquireCodePageWithCapacity /disk/wasm3/source/m3_env.c:1058:20
    #4 0x55de910fff78 in EnsureCodePageNumLines /disk/wasm3/source/m3_compile.c:34:28
    #5 0x55de910b2d8e in Compile_BranchTable /disk/wasm3/source/m3_compile.c:1546:1
    #6 0x55de910f6b8c in CompileBlockStatements /disk/wasm3/source/m3_compile.c:2608:1
    #7 0x55de910face1 in CompileFunction /disk/wasm3/source/m3_compile.c:2899:1
    #8 0x55de9110b1f2 in m3_FindFunction /disk/wasm3/source/m3_env.c:729:1
    #9 0x55de91096f8c in repl_call /disk/wasm3/platforms/app/main.c:256:23
    #10 0x55de91099be0 in main /disk/wasm3/platforms/app/main.c:636:26
    #11 0x7fb47abc730f in __libc_start_call_main libc-start.c

SUMMARY: AddressSanitizer: heap-buffer-overflow /disk/wasm3/source/m3_code.c:25:29 in NewCodePage
Shadow bytes around the buggy address:
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa 00 fa fa fa 04 fa fa fa 00 00 fa fa 01 fa
=>0x0c047fff8010:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8060: 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
==43773==ABORTING
```

zu1k commented on Apr 15

Author

@vshymanskyy Could you please confirm this?

vshymanskyy commented on Jul 12 Member

Related to #344 ?

vshymanskyy closed this as completed on Aug 29

Assignees

No one assigned

Labels

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants