

New issue

[Jump to bottom](#)

# SEGV njs\_vmcode.c:802:27 in njs\_vmcode\_interpreter #483

✓ Closed    Q1IQ opened this issue on Mar 2 · 0 comments

Assignees



Labels

bug    fuzzer

Q1IQ commented on Mar 2

## Environment

```
OS      : Linux ubuntu 5.13.0-27-generic #29~20.04.1-Ubuntu SMP Fri Jan 14 00:32:30 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
Commit  : f65981b0b8fcf02d69a40bc934803c25c9f607ab
Version : 0.7.2
Build   :
        NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
        NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

## Proof of concept

```
function main() {
  const a4 = Promise["race"]([Float64Array]);
  function a14(a15,a16) {
    const a17 = async (a18,a19) => {
      const a20 = await a15;
      for (const a22 in "test") {
      }
    };
    const a23 = a17();
  }
  const a24 = a14(a4);
}
main();
```

## Stack dump

AddressSanitizer:DEADLYSIGNAL

=====

==732128==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004e3e53 bp 0x7ffe6e1f76b0 sp 0x7ffe6e1f6e80 T0)

==732128==The signal is caused by a READ memory access.

==732128==Hint: this fault was caused by a dereference of a high value address (see register values below). Dissassemble the provided pc to learn which register was used.

```
#0 0x4e3e53 in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:802:27
#1 0x6050bc in njs_await_fulfilled
/home/q1iq/Documents/origin/njs_f65981b/src/njs_async.c:96:11
#2 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
#3 0x53b029 in njs_function_frame_invoke
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:777:16
#4 0x53b029 in njs_function_call2
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:600:11
#5 0x5f45b7 in njs_function_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.h:180:12
#6 0x5f45b7 in njs_promise_reaction_job
/home/q1iq/Documents/origin/njs_f65981b/src/njs_promise.c:1171:15
#7 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
#8 0x4deb20 in njs_vm_invoke /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:440:12
#9 0x4deb20 in njs_vm_call /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:424:12
#10 0x4deb20 in njs_vm_handle_events
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:584:19
#11 0x4deb20 in njs_vm_run /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:544:12
#12 0x4c82d7 in njs_process_script
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:924:15
#13 0x4c73a1 in njs_process_file
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:619:11
#14 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
#15 0x7f3e31cf00b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
#16 0x41dabd in _start (/home/q1iq/Documents/origin/njs_f65981b/build/njs+0x41dabd)
```

AddressSanitizer can not provide additional info.


SUMMARY: AddressSanitizer: SEGV /home/q1iq/Documents/origin/njs\_f65981b/src/njs\_vmcode.c:802:27 in njs\_vmcode\_interpreter

==732128==ABORTING

## Credit

Q1IQ(@Q1IQ)

  **xeioex** self-assigned this on Apr 22

 **nginx-hg-mirror** closed this as completed in [31ed93a](#) on Apr 26

---

#### Assignees

 **xeioex**

---

#### Labels

**bug** **fuzzer**

---

#### Projects

None yet

---

#### Milestone

No milestone

---

#### Development

No branches or pull requests

---

#### 2 participants

