SEGV in njs_promise_reaction_job #533

Closed Q1IQ1337 opened this issue on Jun 3 · 0 comments

Labels bug fuzzer

Q1IQ1337 commented on Jun 3 • edited by xeioex

Environment

```
OS      : Linux ubuntu 5.13.0-44-generic #49~20.04.1-Ubuntu SMP Wed May 18 18:44:28 UTC 2022
x86_64 x86_64 x86_64 GNU/Linux
Commit  : d09868bc71f9a990445959329ad8c1b10d3898f5
Version : 0.7.4
Build   :
          NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
          NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

Proof of concept

```
async function f(a1,a2) {
    var v = await a1;
}

f.bind(1,2)();
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3153028==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000103 (pc 0x0000004e4e0e bp
0x7ffd69615960 sp 0x7ffd696150c0 T0)
==3153028==The signal is caused by a READ memory access.
==3153028==Hint: address points to the zero page.
    #0 0x4e4e0e in njs_scope_valid_value /path/to/njs/src/njs_scope.h:86:10
    #1 0x4e4e0e in njs_vmcode_interpreter /path/to/njs/src/njs_vmcode.c:175:17
    #2 0x603263 in njs_await_fulfilled /path/to/njs/src/njs_async.c:91:11
    #3 0x53afac in njs_function_native_call /path/to/njs/src/njs_function.c:728:11
    #4 0x539699 in njs_function_frame_invoke /path/to/njs/src/njs_function.c:766:16
    #5 0x539699 in njs_function_call2 /path/to/njs/src/njs_function.c:592:11
    #6 0x5f2727 in njs_function_call /path/to/njs/src/njs_function.h:178:12
    #7 0x5f2727 in njs_promise_reaction_job /path/to/njs/src/njs_promise.c:1171:15
    #8 0x53afac in njs_function_native_call /path/to/njs/src/njs_function.c:728:11
    #9 0x4dde50 in njs_vm_invoke /path/to/njs/src/njs_vm.c:428:12
    #10 0x4dde50 in njs_vm_call /path/to/njs/src/njs_vm.c:412:12
    #11 0x4dde50 in njs_vm_handle_events /path/to/njs/src/njs_vm.c:572:19
    #12 0x4dde50 in njs_vm_run /path/to/njs/src/njs_vm.c:532:12
    #13 0x4c7fd7 in njs_process_script /path/to/njs/src/njs_shell.c:924:15
    #14 0x4c71eb in njs_process_file /path/to/njs/src/njs_shell.c:619:11
    #15 0x4c71eb in main /path/to/njs/src/njs_shell.c:303:15
    #16 0x7f4ec0d9e082 in __libc_start_main /build/glibc-KZwQYS/glibc-2.31/csu/../csu/libc-
start.c:308:16
    #17 0x41da7d in _start (/path/to/njs/build/njs+0x41da7d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /path/to/njs/src/njs_scope.h:86:10 in njs_scope_valid_value
==3153028==ABORTING
```

xeioex added bug **fuzzer** labels on Jun 3

This was referenced on Sep 27

SEGV in njs_vmcode_interpreter in njs_vmcode.c:1037:21 #579

Closed

SEGV src/njs_lvlhsh.c:203:12 in njs_lvlhsh_level_find #546

Closed

nginx-hg-mirror closed this as completed in `e55edc6` on Oct 10

xeioex mentioned this issue on Oct 18

SEGV njs_vmcode.c:2140:5 in njs_vmcode_try_start #586

Closed

Assignees

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants