New issue

Jump to bottom

SEGV njs_value.c:1083:19 in njs_value_property #504

Closed **dramthy** opened this issue on May 19 · 0 comments

Labels bug fuzzer

dramthy commented on May 19 • edited by xeioex

Environment

```
Commit  : 6cef7f5055ec24275f0ae121c7f8709ff3e0c454
Version : 0.7.4
Build   :
     ./configure --cc=clang --address-sanitizer=YES
     make
```

Proof of concept

```
// minified
function f() {}
Object.defineProperty(f, 'length', {set: () => {}});
Object.defineProperty(f, 'length', Object.getOwnPropertyDescriptor([], 'length'));
f.length
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==25984==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004ea634 bp 0x7ffdd4213270 sp
0x7ffdd42130c0 T0)
==25984==The signal is caused by a READ memory access.
==25984==Hint: this fault was caused by a dereference of a high value address (see register values
below).  Disassemble the provided pc to learn which register was used.
    #0 0x4ea634 in njs_value_property /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_value.c:1083:19
```

```
    #1 0x521273 in njs_object_length /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_object.c:2628:11
    #2 0x600a64 in njs_promise_race /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_promise.c:1727:11
    #3 0x54c08e in njs_function_native_call /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_function.c:728:11
    #4 0x54a9a7 in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_function.c:766:16
    #5 0x4f9b4f in njs_vmcode_interpreter /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_vmcode.c:799:23
    #6 0x54b526 in njs_function_lambda_call /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_function.c:693:11
    #7 0x54a9b9 in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_function.c:769:16
    #8 0x4f9b4f in njs_vmcode_interpreter /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_vmcode.c:799:23
    #9 0x4f25ba in njs_vm_start /home/ubuntu/njs-fuzz/JSEngine/njs-asan/src/njs_vm.c:541:11
    #10 0x4de3fd in njs_process_script /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_shell.c:890:19
    #11 0x4dd98f in njs_process_file /home/ubuntu/njs-fuzz/JSEngine/njs-
asan/src/njs_shell.c:619:11
    #12 0x4dd98f in main /home/ubuntu/njs-fuzz/JSEngine/njs-asan/src/njs_shell.c:303:15
    #13 0x7f7bafed2082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) (BuildId:
1878e6b475720c7c51969e69ab2d276fae6d1dee)
    #14 0x41ea5d in _start (/home/ubuntu/njs-fuzz/JSEngine/njs-asan/build/njs+0x41ea5d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/ubuntu/njs-fuzz/JSEngine/njs-asan/src/njs_value.c:1083:19 in
njs_value_property
==25984==ABORTING
```

Credit
dramthy(**@topsec** alpha)

dramthy changed the title ~~**SEGV njs_value.c:1083:19 in njs_value_property**~~ **SEGV njs_value.c:1083:19 in njs_value_property #bug #fuzzer** on May 19

dramthy changed the title ~~**SEGV njs_value.c:1083:19 in njs_value_property #bug #fuzzer**~~ **SEGV njs_value.c:1083:19 in njs_value_property** on May 19

xeioex added bug **fuzzer** labels on May 19

This was referenced on May 19

SEGV njs_object_prop.c:420:23 in njs_object_prop_define #501

Closed

SEGV njs_object_prop.c:739:19 in njs_object_prop_descriptor #502

Closed

nginx-hg-mirror closed this as completed in 6549d49 on May 19

Assignees

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants