

New issue

[Jump to bottom](#)

SEGV njs_array.c:335:41 in njs_array_add #471

🔒 Closed Q1IQ opened this issue on Feb 15 · 0 comments

Labels bug fuzzer

Q1IQ commented on Feb 15 • edited by xeioex ▼

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  : 7bd570b39297d3d91902c93a624c89b08be7a6fe
Version : 0.7.2
Build   :
        NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
        NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

Proof of concept

```
const a1 = [1];
a1[1111111] = 2;
[3].concat(a1,[4])
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=====
==2064573==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000080 (pc 0x7fe5e5c03c63 bp
0x7fff0c41ad10 sp 0x7fff0c41a4c8 T0)
==2064573==The signal is caused by a WRITE memory access.
==2064573==Hint: address points to the zero page.
      #0 0x7fe5e5c03c63 in memcpy /build/glibc-eX1tMB/glibc-
2.31/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:144
```


```
#1 0x495737 in __asan_memcpy (/home/q1iq/Documents/origin/njs/build/njs+0x495737)
#2 0x51ff27 in njs_array_add /home/q1iq/Documents/origin/njs/src/njs_array.c:335:41
#3 0x51ff27 in njs_array_prototype_concat
/home/q1iq/Documents/origin/njs/src/njs_array.c:1757:27
#4 0x53bf9c in njs_function_native_call
/home/q1iq/Documents/origin/njs/src/njs_function.c:739:11
#5 0x4e47fa in njs_vmcode_interpreter /home/q1iq/Documents/origin/njs/src/njs_vmcode.c:785:23
#6 0x53b43a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs/src/njs_function.c:703:11
#7 0x4e47fa in njs_vmcode_interpreter /home/q1iq/Documents/origin/njs/src/njs_vmcode.c:785:23
#8 0x4deb7b in njs_vm_start /home/q1iq/Documents/origin/njs/src/njs_vm.c:493:11
#9 0x4c8099 in njs_process_script /home/q1iq/Documents/origin/njs/src/njs_shell.c:903:19
#10 0x4c7484 in njs_process_file /home/q1iq/Documents/origin/njs/src/njs_shell.c:632:11
#11 0x4c7484 in main /home/q1iq/Documents/origin/njs/src/njs_shell.c:316:15
#12 0x7fe5e5b6c0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-
start.c:308:16
#13 0x41dabd in _start (/home/q1iq/Documents/origin/njs/build/njs+0x41dabd)
```

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-eX1tMB/glibc-
2.31/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:144 in memcpy
==2064573==ABORTING

Credit

Q1IQ(@Q1IQ)

  **xeioex** added **bug** **fuzzer** labels on Feb 15

 **nginx-hg-mirror** closed this as completed in [e673ae4](#) on Feb 21

Assignees

No one assigned

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

no milestone

Development

No branches or pull requests

2 participants

