

New issue

[Jump to bottom](#)

SEGV njs_scope.h:85:10 in njs_scope_valid_value #470

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

Assignees



Labels

bug fuzzer

Q1IQ commented on Feb 15

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

```
function main() {
function a0(a1,a2) {
    a0 = a1;
}
a0();
a0();
}
main();
```

Stack dump

AddressSanitizer:DEADLYSIGNAL


```
=====
==2064564==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x0000004e36b5 bp
0x7ffd26e5c130 sp 0x7ffd26e5b920 T0)
==2064564==The signal is caused by a READ memory access.
==2064564==Hint: address points to the zero page.
#0 0x4e36b5 in njs_scope_valid_value /home/q1iq/Documents/origin/njs/src/njs_scope.h:85:10
#1 0x4e36b5 in njs_vmcode_function_copy
/home/q1iq/Documents/origin/njs/src/njs_vmcode.c:1223:14
#2 0x4e36b5 in njs_vmcode_interpreter /home/q1iq/Documents/origin/njs/src/njs_vmcode.c:727:23
#3 0x53b43a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs/src/njs_function.c:703:11
#4 0x4e47fa in njs_vmcode_interpreter /home/q1iq/Documents/origin/njs/src/njs_vmcode.c:785:23
#5 0x53b43a in njs_function_lambda_call
/home/q1iq/Documents/origin/njs/src/njs_function.c:703:11
#6 0x4e47fa in njs_vmcode_interpreter /home/q1iq/Documents/origin/njs/src/njs_vmcode.c:785:23
#7 0x4deb7b in njs_vm_start /home/q1iq/Documents/origin/njs/src/njs_vm.c:493:11
#8 0x4c8099 in njs_process_script /home/q1iq/Documents/origin/njs/src/njs_shell.c:903:19
#9 0x4c7484 in njs_process_file /home/q1iq/Documents/origin/njs/src/njs_shell.c:632:11
#10 0x4c7484 in main /home/q1iq/Documents/origin/njs/src/njs_shell.c:316:15
#11 0x7f135ab960b2 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/build/njs+0x41dabd)
```


AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/q1iq/Documents/origin/njs/src/njs_scope.h:85:10 in
njs_scope_valid_value
==2064564==ABORTING

Credit

Q1IQ(@Q1IQ)

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

 **xeioex** self-assigned this on Jun 1


 **nginx-hg-mirror** closed this as completed in [04f59f9](#) on Jun 2

 **xeioex** mentioned this issue on Jun 2

SEGV njs_scope.h:86:10 in njs_scope_valid_value #529

 Closed

Assignees

 xeioex

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

