

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

SEGV in njs_sprintf.c:424:19 #553

✓ Closed **yype** opened this issue on Jun 20 · 0 comments

Assignees



Labels

bug

yype commented on Jun 20

Hi, the following PoC triggers a crash (related to string fmt?) in the latest commit.

```
(function() {
while ([])
try {
break
try {
return } catch (a) {}
} catch (b) {}
}())
```

Environment:

Commit: e008f7ae22834ff1173b7a0067b14c821102018d
System: Ubuntu 18.04.6 LTS

ASan output:

```
/njs/njs_asan/build/njs ./poc.js
AddressSanitizer:DEADLYSIGNAL
=====
==177164==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000000803 (pc 0x7ffff6807384 bp
0x7fffffb790 sp 0x7fffffa48 T0)
==177164==The signal is caused by a READ memory access.
==177164==Hint: address points to the zero page.
#0 0x7ffff6807384 (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)
#1 0x497d01 in __asan_memcpy (/njs/njs_asan/build/njs+0x497d01)
```


```
#2 0x4d2b96 in njs_vsprintf /njs/njs_asan/src/njs_sprintf.c:424:19
#3 0x541fe6 in njs_error_fmt_new /njs/njs_asan/src/njs_error.c:69:13
#4 0xea1a7 in njs_vmcode_error /njs/njs_asan/src/njs_vmcode.c
#5 0x4e1c7e in njs_vmcode_interpreter /njs/njs_asan/src/njs_vmcode.c:993:17
#6 0x52dcdf in njs_function_lambda_call /njs/njs_asan/src/njs_function.c:693:11
#7 0x52d6d0 in njs_function_frame_invoke /njs/njs_asan/src/njs_function.c:780:16
#8 0x4e39ec in njs_vmcode_interpreter /njs/njs_asan/src/njs_vmcode.c:799:23
#9 0x4ddf17 in njs_vm_start /njs/njs_asan/src/njs_vm.c:539:11
#10 0x4cb35b in njs_process_script /njs/njs_asan/src/njs_shell.c:890:19
#11 0x4cbb68 in njs_process_file /njs/njs_asan/src/njs_shell.c:619:11
#12 0x4ca1fc in main /njs/njs_asan/src/njs_shell.c:303:15
#13 0x7ffff676dc86 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
#14 0x41d9a9 in _start (/njs/njs_asan/build/njs+0x41d9a9)
```


AddressSanitizer can not provide additional info.

SUMMARY: AddressSanitizer: SEGV (/lib/x86_64-linux-gnu/libc.so.6+0xbb384)

==177164==ABORTING

  **xeioex** added the `bug` label on Jun 21

  **xeioex** self-assigned this on Jun 27

 **nginx-hg-mirror** closed this as completed in [4045538](#) on Jun 29

Assignees

 **xeioex**

Labels

`bug`

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

