nginx / **njs** Public

Code Issues 41 Pull requests 2 Actions Security Insights

New issue

Jump to bottom

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

Closed **Q1IQ** opened this issue on Jun 2 · 1 comment

Labels bug duplicate fuzzer

Q1IQ commented on Jun 2 • edited

Environment

```
OS      : Linux ubuntu 5.11.10 #1 SMP Sat Oct 30 23:40:08 CST 2021 x86_64 x86_64 x86_64 GNU/Linux
Commit  : c62a9fb92b102c90a66aa724cb9054183a33a68c
Version : 0.7.4
Build   :
          NJS_CFLAGS="$NJS_CFLAGS -fsanitize=address"
          NJS_CFLAGS="$NJS_CFLAGS -fno-omit-frame-pointer"
```

Proof of concept

```
function main() {
function a2(a3,a4) {
    try {
        var a5 = a2();
        var a6 = {};
        var a7 = [a6,a6,a6,1.0,a6];
        var a16 = a2();
        a2 = a5;
        var a18 = `
            var a20 = (256)();
            var a21 = \`
                var a23 = Object();
                var a24 = a20(...1894060106n,a23,a23,a7,Object,2152566096n);
                var a25 = [Object,2152566096n,a23];
            \`;
            var a26 = {"d":2152566096n};
            var a27 =
{"a":a21,"b":a26,"constructor":1894060106n,"e":a26,"toString":-4207569322n,..."c",...2152566096n,...a
```

```
            var a28 = a20(a21,a27,1894060106n,-4207569322n,2152566096n);
        `;
        var a30 = /./m;
        var a36 = /t/i;
        var a39 = `
            throw 0n;
            var a40 = a36[(0n)](0n);
            var a41 = -4207569322n != -828352779n;
        `;
        var a43 = /dN\w/i;
        var a47 = Object();
        var a48 = `
            var a49 = [a47,a47,2152566096n,a30,a48,256,1894060106n,2152566096n,a30];
            var a51 = a49(0n);
            var a52 = a43["test"](0n);
            var a53 = -1410768346n != 1538778485n;
        `;
    } catch(a54) {
    } finally {
    }
}
var a56 = new Promise(a2);
}
main();
```

Stack dump

```
==3049569==ERROR: UndefinedBehaviorSanitizer: SEGV on unknown address 0x000000000000 (pc 0x000000435e70 bp 0x7ffc22356800 sp 0x7ffc22356620 T3049569)
==3049569==The signal is caused by a READ memory access.
==3049569==Hint: address points to the zero page.
    #0 0x435e70 in njs_scope_valid_value /njs/src/njs_scope.h:86:10
    #1 0x435e70 in njs_vmcode_function_copy /njs/src/njs_vmcode.c:1262:14
    #2 0x435e70 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:741:23
    #3 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #4 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #5 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #6 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #7 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #8 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #9 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #10 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #11 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #12 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #13 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #14 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #15 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #16 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #17 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #18 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #19 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #20 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #21 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #22 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #23 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #24 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #25 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #26 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #27 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #28 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #29 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #30 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #31 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #32 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #33 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #34 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #35 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #36 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #37 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #38 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #39 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #40 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #41 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #42 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #43 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #44 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #45 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #46 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #47 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #48 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #49 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #50 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #51 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #52 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #53 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #54 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #55 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #56 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #57 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #58 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #59 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #60 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #61 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #62 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #63 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #64 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #65 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #66 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #67 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #68 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #69 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #70 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #71 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #72 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #73 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #74 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #75 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #76 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #77 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #78 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #79 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #80 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #81 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #82 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #83 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #84 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #85 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #86 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #87 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #88 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #89 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #90 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #91 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #92 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #93 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #94 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #95 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #96 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #97 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #98 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #99 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #100 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #101 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #102 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #103 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #104 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #105 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #106 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #107 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #108 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #109 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #110 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #111 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #112 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #113 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #114 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #115 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #116 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #117 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #118 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #119 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #120 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #121 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #122 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #123 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #124 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #125 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #126 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #127 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #128 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #129 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #130 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #131 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #132 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #133 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #134 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #135 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #136 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #137 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #138 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #139 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #140 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #141 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #142 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #143 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #144 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #145 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #146 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #147 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #148 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #149 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #150 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #151 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #152 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #153 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #154 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #155 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #156 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #157 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #158 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #159 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #160 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #161 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #162 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #163 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #164 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #165 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #166 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #167 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #168 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #169 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #170 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #171 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #172 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #173 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #174 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #175 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #176 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #177 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #178 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #179 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #180 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #181 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #182 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #183 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #184 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #185 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #186 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #187 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #188 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #189 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #190 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #191 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #192 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #193 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #194 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #195 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #196 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #197 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #198 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #199 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #200 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #201 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #202 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #203 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #204 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #205 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #206 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #207 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #208 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #209 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #210 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #211 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #212 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #213 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #214 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #215 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #216 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #217 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #218 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #219 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #220 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #221 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #222 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #223 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #224 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #225 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #226 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #227 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #228 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #229 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #230 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #231 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #232 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #233 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #234 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #235 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #236 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #237 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #238 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #239 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #240 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #241 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #242 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #243 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #244 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #245 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #246 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #247 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #248 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #249 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #250 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23
    #251 0x468070 in njs_function_lambda_call /njs/src/njs_function.c:693:11
    #252 0x4364d7 in njs_vmcode_interpreter /njs/src/njs_vmcode.c:799:23

UndefinedBehaviorSanitizer can not provide additional info.
SUMMARY: UndefinedBehaviorSanitizer: SEGV /njs/src/njs_scope.h:86:10 in njs_scope_valid_value
```

Credit

Q1IQ(**@Q1IQ**)

xeioex commented on Jun 2 Contributor

Duplicate of #470.

xeioex closed this as completed on Jun 2

xeioex added bug **duplicate** **fuzzer** labels on Jun 2

Assignees

No one assigned

Labels

bug **duplicate** **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

No branches or pull requests

2 participants