New issue

Jump to bottom

SEGV src/njs_djb_hash.c:21:16 in njs_djb_hash #540

Closed **dramthy** opened this issue on Jun 9 · 0 comments

Labels bug fuzzer

dramthy commented on Jun 9

Environment

```
Commit  : c756e23eb09dac519fe161c88587cc034306630f (high:1882)
Version : 0.7.5
Build   :
     ./configure --cc=clang --address-sanitizer=YES
     make
```

Proof of concept

```
// Minimizing 8AC3654E-F5A1-405C-B380-951904AD058C
function placeholder(){}
function main() {
var v1 = Function;
var v6 = [930866.8987935185,930866.8987935185,930866.8987935185,930866.8987935185];
var v8 = [v6,1050462187];
var v11 = [930866.8987935185,930866.8987935185,930866.8987935185,930866.8987935185];
var v13 = [v11,1050462187];
var v15 = v11.__proto__;
function v16(v17,v18,v19,...v20) {
    var v21 = [v17,-1000000000000.0];
    function v22(v23,v24,v25,...v26) {
        var v27 = {"d":v22};
        var v28 = Object.defineProperty(v15,v18,v27);
    }
    var v30 = v21["find"](v22);
}
var v32 = v13["find"](v16);
var v34 = v6.__proto__;
function v35(v36,v37,v38,...v39) {
    'use strict';
```

```
    var v40 = [v36,-1000000000000.0];
    var v42 = 471270.459031428 in v39;
    var v43 = 1000.0;
    var v45 = String.fromCodePoint();
    var v46 = -128;
    var v50 = `YVySS90U8G${v45}string${-452883207}-2${Uint8Array}dotAll`.indexOf();
    var v51 = 50691;
    var v52 = 658545.3967616097;
    var v53 = undefined;
    var v54 = -1.7976931348623157e+308;
    var v55 = 2147483647;
    var v56 = 4184750072;
    var v57 = "toString";
    var v58 = Float64Array;
    var v59 = "a";
    var v60 = 54444;
    var v61 = ["c14RHVOudV",1050462187];
    function v62(v63,v64,v65,...v66) {
        var v68 = v34["shift"]();
    }
    var v70 = v61["find"](v62);
    function v71(v72,v73,v74,...v75) {
        'use strict';
        var v76 = {"get":v71};
        var v77 = Object.defineProperty(v34,35017,v76);
    }
    var v79 = v40["find"](v71);
}
var v81 = v8["find"](v35);
}
main();
// CRASH INFO
// ==========
// TERMSIG: 11
// STDERR:
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2802==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004e312b bp 0x7ffca2668c70 sp
0x7ffca2668c40 T0)
==2802==The signal is caused by a READ memory access.
==2802==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 0x4e312b in njs_djb_hash /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_djb_hash.c:21:16
    #1 0x4f10cb in njs_property_query /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_value.c:618:32
    #2 0x502d6a in njs_vmcode_property_in /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:1431:11
    #3 0x502d6a in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:492:23
    #4 0x574b62 in njs_function_lambda_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:693:11
    #5 0x573a55 in njs_function_frame_invoke /home/ubuntu/njs-
```

```
fuzz/JSEngine/njs/src/njs_function.c:780:16
    #6 0x573a55 in njs_function_call2 /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.c:592:11
    #7 0x560b05 in njs_function_call /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_function.h:178:12
    #8 0x560b05 in njs_array_iterator_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_array.c:1918:12
    #9 0x560b05 in njs_array_handler_find /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_array.c:2025:11
    #10 0x65b9ea in njs_object_iterate /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_iterator.c
    #11 0x554e0f in njs_array_prototype_iterator /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_array.c:2297:11
    #12 0x57599e in njs_function_native_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:739:11
    #13 0x573d0c in njs_function_frame_invoke /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:777:16
    #14 0x500f5f in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:799:23
    #15 0x574b62 in njs_function_lambda_call /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:693:11
    #16 0x573d3f in njs_function_frame_invoke /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_function.c:780:16
    #17 0x500f5f 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 0x4ddbe8 in main /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:483:15
    #22 0x7f1db1e4a082 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_djb_hash.c:21:16 in
njs_djb_hash
==2802==ABORTING
```

Credit
dramthy(**@topsec** alpha)

 **xeioex** added bug **fuzzer** labels on Jun 10

 This was referenced on Jun 11

SEGV njs/src/njs_scope.h:74:12 in njs_scope_value #541

Closed

SEGV src/njs_async.c:73:21 in njs_await_fulfilled #539

Closed

nginx-hg-mirror closed this as completed in `7b3fba5` on Jun 11

Assignees

No one assigned

Labels

bug **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants