<> Code   ⊙ Issues   41   ⑂ Pull requests   2   ▷ Actions   🛡 Security   ∿ Insights

New issue

SEGV njs_scope.h:74:12 Out-of-bounds Read in njs_scope_value #506

⊘ Closed   **dramthy** opened this issue on May 29 · 2 comments

Assignees

Labels   bug   **fuzzer**

---

dramthy commented on May 29 · edited by xeioex ▾

Environment

```
Commit  : 9f4ebc96148308a8ce12f2b54432c87e6d78b881
Version : 0.7.4
Build   :
     ./configure --cc=clang --address-sanitizer=YES
     make
```

Proof of concept

```
// Minimizing 34F6ED23-C193-452B-B724-E62BD7E15360
function placeholder(){}
function main() {
function v0(v1,v2,v3,v4,...v5) {
    try {
        async function v7(v8,v9,v10,v11) {
            var v12 = await Proxy;
        }
        var v13 = v0();
    } catch(v14) {
    } finally {
    }
    var v15 = {};
    var v16 = /gL8?/;
    var v17 = {};
    var v18 = [v15,v17,v16];
    function v20(v21) {
```

```
            v18[1866532165] = Map;
        }
        async function v24(v25,v26) {
            var v27 = await Map;
        }
        function v28(v29,v30) {
        }
        var v32 = new Promise(v28);
        var v34 = v32["catch"]();
        var v37 = {"get":Promise,"set":v24};
        var v38 = Object.defineProperty(v34,"constructor",v37);
        async function v39(v40,v41) {
            var v42 = await v38;
        }
        var v43 = v39();
        var v44 = v20(Map);
    }
    var v45 = v0();
    }
    main();
```

Minified

```
function run_then() {}

function f(n) {
    if (n == 2) {
        return;
    }

    try {
        f(n + 1);
    } catch(e) {
    }


    var p = new Promise(run_then);
    Object.defineProperty(p, "constructor", {get: () => ({}).a.a});
    async function g() {
        await p;
    }

    g();

    throw 'QQ';
}

f(0);
```

Stack dump

```
AddressSanitizer:DEADLYSIGNAL
================================================================
```

```
==815==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000040 (pc 0x0000004ff20b bp
0x7ffc7abf6030 sp 0x7ffc7abf5880 T0)
==815==The signal is caused by a READ memory access.
==815==Hint: address points to the zero page.
    #0 0x4ff20b in njs_scope_value /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_scope.h:74:12
    #1 0x4ff20b in njs_scope_valid_value /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_scope.h:84:13
    #2 0x4ff20b in njs_vmcode_interpreter /home/ubuntu/njs-
fuzz/JSEngine/njs/src/njs_vmcode.c:155:13
    #3 0x4fa5ae in njs_vm_start /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_vm.c:541:11
    #4 0x4df3fb in njs_process_script /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:1132:19
    #5 0x4e007f in njs_process_file /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:836:11
    #6 0x4ddbe8 in main /home/ubuntu/njs-fuzz/JSEngine/njs/src/njs_shell.c:483:15
    #7 0x7f8dc7694082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x24082) (BuildId:
1878e6b475720c7c51969e69ab2d276fae6d1dee)
    #8 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_scope.h:74:12 in
njs_scope_value
==815==ABORTING
```

Credit
dramthy(@**topsec** alpha)

✏️ 🤖 **dramthy** changed the title ~~SEGV njs_scope.h:74:12 Heap-based Buffer Overflow in njs_scope_value~~
SEGV njs_scope.h:74:12 Out-of-bounds Read in njs_scope_value on May 29

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

👤 🌐 **xeioex** self-assigned this on Jun 1

↗️ This was referenced on Jun 1

SEGV njs_error.c:1303:39 in njs_add_backtrace_entry #508
(⊘ Closed)

SEGV njs_function.c:443:13 in njs_function_lambda_frame #509
(⊘ Closed)

SEGV njs_function.c:457:42 in njs_function_lambda_frame #510
(⊘ Closed)

SEGV njs_function.c:720:13 in njs_function_native_call #511

SEGV src/njs_function.c:880:5 in njs_function_capture_closure #512

SEGV src/njs_function.c:880:19 in njs_function_capture_closure #513

SEGV src/njs_function.h:167:5 in njs_function_previous_frame #514

---

xeioex commented on Jun 1   Contributor

The patch

```
# HG changeset patch
# Parent   d63163569c25cb90fe654f0fedefde43553f833a
Fixed njs_vmcode_interpreter() when await fails.

Previously, while interpreting a user function, njs_vmcode_interpreter()
might return prematurely when an error happens in await instruction.
This is not correct because the current frame has to be unwound (or
exception caught) first.

The fix is exit through only 5 appropriate exit points to ensure
proper unwinding.

The patch correctly fixes issue reported in 07ef6c1f04f1 (0.7.3).

This closes #506 issue on Github.

diff --git a/src/njs_vmcode.c b/src/njs_vmcode.c
--- a/src/njs_vmcode.c
+++ b/src/njs_vmcode.c
@@ -858,7 +858,12 @@ next:

                njs_vmcode_debug(vm, pc, "EXIT AWAIT");

-               return njs_vmcode_await(vm, await, promise_cap, async_ctx);
+               ret = njs_vmcode_await(vm, await, promise_cap, async_ctx);
+               if (njs_slow_path(ret == NJS_ERROR)) {
+                   goto error;
+               }
+
+               return ret;

            case NJS_VMCODE_TRY_START:
                ret = njs_vmcode_try_start(vm, value1, value2, pc);
@@ -1923,6 +1928,7 @@ njs_vmcode_await(njs_vm_t *vm, njs_vmcod

    value = njs_scope_valid_value(vm, await->retval);
```

```
        if (njs_slow_path(value == NULL)) {
+           njs_internal_error(vm, "await->retval is invalid");
            return NJS_ERROR;
        }
```

SEGV src/njs_lvlhsh.c:176:16 in njs_lvlhsh_find #515

⊘ Closed

SEGV src/njs_lvlhsh.c:231:17 in njs_lvlhsh_bucket_find #516

⊘ Closed

SEGV src/njs_number.c:1097:13 in njs_number_parse_int #518

⊘ Closed

SEGV src/njs_object.c:2136:24 in njs_object_set_prototype #519

⊘ Closed

SEGV src/njs_string.c:2531:13 in njs_string_offset #520

⊘ Closed

SEGV njs/src/njs_utf8.c:119:9 in njs_utf8_decode #521

⊘ Closed

SEGV src/njs_value.c:241:41 in njs_value_own_enumerate #525

⊘ Closed

SEGV src/njs_vmcode.c:1006:37 in njs_vmcode_interpreter #526

⊘ Closed

SEGV src/njs_vmcode.c:1839:22 in njs_vmcode_return #527

⊘ Closed

SEGV src/njs_vmcode.c:2123:9 in njs_vmcode_finally #528

⊘ Closed

dramthy commented on Jun 1 • edited ▾   Author

Yes, I check the patch is valid for
#506,#508,#509,#510,#511,#512,#513,#514,#515,#516,#518,#519,#520,#521,#525,#526,#527,#528. **@xeioex**

nginx-hg-mirror closed this as completed in `d09868b` on Jun 2

⤴ 🔧 **dramthy** mentioned this issue on Jun 9

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

⊘ **Closed**

Assignees

🖼 **xeioex**

Labels

bug   **fuzzer**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants

🖼 🔧