

New issue

Jump to bottom

stack overflow #11

Closed rain6851 opened this issue on Apr 14, 2020 · 3 comments

rain6851 commented on Apr 14, 2020 • edited

Enviroment

operating system: ubuntu18.04  
compile command: make CONFIG\_ASAN=y  
test command: ./qjs poc

poc:

```
let x = 'foo';  
const y = { z: 0 };  
const a = './ode_FIXTURE.js';  
const b = './moFIXTURE.js';  
async function fn() {  
  var e8ZE = fn();  
  fn();  
}  
var THdX = fn();  
var DakD = unescape('f5~1~n1');
```

crash location:

```
?0x7ffff6e8c7e9 push r12  
0x7ffff6e8c7eb mov r13, rdx  
0x7ffff6e8c7ee push rbp  
0x7ffff6e8c7ef push rbx  
0x7ffff6e8c7f0 sub rsp, 0x78  
0x7ffff6e8c7f4 mov rax, QWORD PTR fs:0x28  
? threads  
[#0] Id 1, Name: "qjs", stopped 0x7ffff6e8c7e9 in ?? (), reason: SIGSEGV  
? trace  
[#0] 0x7ffff6e8c7e9 ?push r12  
[#1] 0x7ffff6f025d3 ?malloc()  
[#2] 0x474db2 ?js_def_malloc(s=0x61600000fca0, size=)  
[#3] 0x47fa17 ?js_malloc_rt()  
[#4] 0x47fa17 ?js_malloc(ctx=0x61500000fd00, size=)  
[#5] 0x73904c ?js_new_shape2.constprop.82(ctx=0x61500000fd00, proto=0x60700000df40, prop_size=0x2, hash_size=0x4)  
[#6] 0x613df0 ?js_new_shape()  
[#7] 0x613df0 ?JS_NewObjectProtoClass(ctx=0x61500000fd00, proto_val={
```

vulnerability description:

ASAN:SIGSEGV

[illegible]

[illegible]

[illegible]

#278 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#279 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#280 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#281 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#282 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#283 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#284 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#285 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#286 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#287 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#288 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#289 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#290 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#291 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#292 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#293 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#294 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#295 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#296 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#297 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#298 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#299 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#300 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#301 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#302 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#303 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#304 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#305 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#306 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#307 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#308 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#309 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#310 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800  
#311 0x40ca81 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:15687  
#312 0x40d0d6 in JS\_CallInternal.lto\_priv.279 /home/node/xQuickJS/quickjs.c:16056  
#313 0x5e202f in async\_func\_resume /home/node/xQuickJS/quickjs.c:18367  
#314 0x5e202f in js\_async\_function\_resume /home/node/xQuickJS/quickjs.c:18693  
#315 0x5e352a in js\_async\_function\_call.lto\_priv.565 /home/node/xQuickJS/quickjs.c:18800

SUMMARY: AddressSanitizer: stack-overflow ??:0 malloc  
==101779==ABORTING

  **rain6851** mentioned this issue on Apr 14, 2020

**heap overflow #10**

 Closed

  **rain6851** mentioned this issue on Apr 23, 2020

**stack overflow #9**

 Closed

**ldarren** commented on May 2, 2020

Owner

node gave infinite recursion, and qjs gave segmentation fault error.  
what is the expected results?

**rain6851** commented on May 3, 2020

Author


node gave infinite recursion, and qjs gave segmentation fault error.  
what is the expected results?

QuickJS should detect this problem like other large JavaScript parsers, report an error, and terminate execution.

**ldarren** commented on Jul 8, 2020

Owner

@rain6851 resolved in 2020-07-05 release

 **ldarren** closed this as completed on Jul 8, 2020

  **kvenux** mentioned this issue on Sep 10, 2020

**stack-overflow at quickjs.c:31754 #29**

 Closed

Assignees

No one assigned

Labels

None yet

---

Projects

None yet

---

Milestone

No milestone

---

Development

No branches or pull requests

---

2 participants

