Jump to bottom

# stack overflow #11



New issue

⊙ 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 = 'too';
const y = { z: 0 };
const a = './ode_FIXTURE.js';
const b = './moFIXTURE.js';
async function fn() {
       var eBZE = fn();
fn();
var THdX = fn();
var DakD = unescape('f5~=1~nl');
```

#### 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 ?¾malloc()

[#2] 0x474db2 ?¾js\_def\_malloc(s=0x61600000fca0, size=)

[#3] 0x47fa17 ?¾js\_malloc\_rt()

[#4] 0x47fa17 ?Řjs\_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 ?ÄJS\_NewObjectProtoClass(ctx=0x61500000fd00, proto\_val={

## vulnerability description:

### ASAN:SIGSEGV

```
==101779==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd517ebfb8 (pc 0x7fc841b28568 bp 0x7ffd517ec800 sp 0x7ffd517ebfa0 T0)
#0 0x7fc841b28567 in malloc (/usr/lib/x86 64-linux-gnu/libasan.so.2+0x98567)
#1 0x43d87c in js def malloc/home/node/xQuickJS/quickjs.c:1567
#2 0x445b6c in js malloc rt /home/node/xQuickJS/quickjs.c:1220
#3 0x445b6c in js_mallocz_rt /home/node/xQuickJS/quickjs.c:1241
#4 0x445b6c in js_mallocz /home/node/xQuickJS/quickjs.c:1272
#5 0x5e2a79 in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18779
#6 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#7 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#8 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#9 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#10 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#11 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#12 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#13 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#14 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#15 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#16 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#17 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickjs.c:16056
#18 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#19 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#20 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#21 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#22 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#23 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#24 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#25 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#26 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#27 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#28 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#29 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#30 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#31 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#32 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#33 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#34 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#35 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#36 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#37 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#38 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#39 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#40 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#41 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#42 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#43 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#44 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#45 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#46 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#47 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#48 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#49 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#50 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#51 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#52 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#53 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#54 0x5e202f in is async function resume /home/node/xQuickJS/quickis.c:18693
#55 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#56 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#57 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#58 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#59 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#60 0x5e352a in is async function call.lto priv.565 /home/node/xQuickJS/quickis.c:18800
#61 0x40ca81 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:15687
#62 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#63 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#64 0x5e202f in is async function resume /home/node/xQuickJS/quickis.c:18693
#65 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#66 0x40ca81 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:15687
#67 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#68 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#69 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#70 0x5e352a in is async function call.lto priv.565 /home/node/xQuickJS/quickis.c:18800
#71 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#72 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#73 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#74 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#75 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#76 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#77 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#78 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#79 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#80 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#81 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#82 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#83 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#84 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#85 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#86 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#87 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#88 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#89 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#90 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#91 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
```

```
#92 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#93 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#94 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#95 0x5e352a in js async function call.lto priv.565 /home/node/xQuickJS/quickjs.c:18800
#96 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#97 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickjs.c:16056
#98 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#99 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#100 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#101 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#102 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#103 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#104 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#105 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#106 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#107 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#108 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#109 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#110 0x5e352a in js async function call.lto priv.565 /home/node/xQuickJS/quickjs.c:18800
#111 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#112 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickjs.c:16056
#113 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#114 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#115 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#116 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#117 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#118 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#119 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#120 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#121 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#122 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#123 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#124 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#125 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#126 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#127 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#128 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#129 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#130 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#131 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#132 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#133 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#134 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#135 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#136 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#137 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#138 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#139 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#140 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#141 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#142 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#143 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#144 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#145 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#146 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#147 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#148 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#149 0x5e202f in is asvnc function resume /home/node/xQuickJS/quickis.c:18693
#150 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#151 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#152 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xOuickJS/quickis.c:16056
#153 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#154 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#155 0x5e352a in is async function call.lto priv.565 /home/node/xQuickJS/quickis.c:18800
#156 0x40ca81 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:15687
#157 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#158 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#159 0x5e202f in is asvnc function resume /home/node/xQuickJS/quickis.c:18693
#160 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#161 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#162 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#163 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#164 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#165 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#166 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#167 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#168 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#169 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#170 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#171 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#172 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#173 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#174 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#175 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#176 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#177 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#178 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#179 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#180 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#181 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#182 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#183 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#184 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
```

```
#185 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#186 0x40ca81 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickjs.c:15687
#187 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickjs.c:16056
#188 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#189 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#190 0x5e352a in js async function call.lto priv.565 /home/node/xQuickJS/quickjs.c:18800
#191 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#192 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#193 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#194 0x5e202f in js async function resume /home/node/xQuickJS/quickjs.c:18693
#195 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#196 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#197 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#198 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#199 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#200 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#201 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#202 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#203 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#204 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#205 0x5e352a in js async function call.lto priv.565 /home/node/xQuickJS/quickjs.c:18800
#206 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#207 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#208 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#209 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#210 0x5e352a in js async function call.lto priv.565 /home/node/xQuickJS/quickjs.c:18800
#211 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#212 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#213 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#214 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#215 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#216 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#217 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#218 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#219 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#220 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#221 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#222 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#223 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#224 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#225 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#226 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#227 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#228 0x5e202f in async func resume /home/node/xQuickJS/quickjs.c:18367
#229 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#230 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#231 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#232 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#233 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#234 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#235 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#236 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#237 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#238 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#239 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#240 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#241 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#242 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#243 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#244 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#245 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#246 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#247 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#248 0x5e202f in async func resume /home/node/xQuickJS/quickis.c:18367
#249 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#250 0x5e352a in is async function call.lto priv.565 /home/node/xQuickJS/quickis.c:18800
#251 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#252 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#253 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#254 0x5e202f in is asvnc function resume /home/node/xQuickJS/quickis.c:18693
#255 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#256 0x40ca81 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:15687
#257 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#258 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#259 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#260 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#261 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#262 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#263 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#264 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#265 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#266 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#267 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
#268 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#269 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#270 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#271 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#272 0x40d0d6 in JS CallInternal.lto priv.279 /home/node/xQuickJS/quickis.c:16056
#273 0x5e202f in async_func_resume /home/node/xQuickJS/quickjs.c:18367
#274 0x5e202f in js_async_function_resume /home/node/xQuickJS/quickjs.c:18693
#275 0x5e352a in js_async_function_call.lto_priv.565 /home/node/xQuickJS/quickjs.c:18800
#276 0x40ca81 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:15687
#277 0x40d0d6 in JS_CallInternal.lto_priv.279 /home/node/xQuickJS/quickjs.c:16056
```

#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 Owner Idarren commented on May 2, 2020 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. Idarren commented on Jul 8, 2020 Owner @rain6851 resolved in 2020-07-05 release p Idarren 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

| Projects<br>None yet                      |  |
|---|--|
| Milestone<br>No milestone                 |  |
| Development  No branches or pull requests |  |

2 participants

