Jump to bottom

## stack overflow #133

rain6851 commented on Apr 17, 2020



New issue

⊙ Closed rain6851 opened this issue on Apr 17, 2020 · 4 comments

```
Enviroment
    operating system: ubuntu18.04 compile command: make build=sanitize
    test command: ./mujs poc
poc:
    est bound function chainnal implementation

* to "collapse" bound funct

/*===
    F() bound foo
object this-F
    string foo
undefined undefined
undefined undefined
    undefined undefined
G() bound bound foo
     object this-F
    string foo
string bar
string quux
     unarg-52
53 string arg-53
    54 string arg-54
55 string arg-55
    56 string arg-56
57 string arg-57
58 string arg-58
59 string arg-59
    60 string arg-60
61 string arg-61
    62 string arg-62
63 string arg-63
64 string arg-64
    65 string arg-65
66 string arg-66
    67 string arg-66
68 string arg-68
69 string arg-69
70 string arg-70
71 string arg-71
    72 string arg-72
    73 string arg-73
74 string arg-74
75 string arg-75
    76 string arg-76
77 string arg-77
    78 string arg-78
79 string arg-79
80 string arg-80
    81 string arg-81
82 string arg-82
    83 string arg-83
    84 string arg-84
85 string arg-85
86 string arg-86
87 string arg-87
88 string arg-88
    89 string arg-89
90 string arg-90
    91 string arg-91
    92 string arg-92
93 string arg-93
    94 string arg-94
95 string arg-95
    96 string arg-96
97 string arg-97
98 string arg-98
     99 string arg-99
    function test() {
            var func;
var F, G, H, I;
            \ensuremath{//} Final function is an ECMAScript function.
            func = function foo(a, b, c, d) {
  print(typeof this, this);
  print(typeof a, a);
  print(typeof b, b);
                    print(typeof c, c);
print(typeof d, d);
```

```
F = func.bind('this-F', 'foo');
    G = F.bind('this-G', 'bar', 'quux');
H = G.bind('this-H', 'baz', 'quuux');
I = G.bind('this-I', 123, 234); // both H and I bind via G
     print('G()', G.name);
     G();
     print('H()', H.name);
     H();
     print('I()', I.name);
     I();
     // Final function is a native function.
     func = Math.max;
     F = func.bind(null):
     G = F.bind(null, 3);
     H = G.bind(null, 4);
     I = H.bind(null, 5);
     print('F()', F.name);
     print(F());
     print('G()', G.name);
    print(G());
print('H()', H.name);
     print(H());
     print('I()', I.name);
     print(I());
     // Lightfunc final target needs testing too; it is covered by {\tt Math.max()}
     // if DUK_USE_LIGHTFUNC_BUILTINS is enabled.
     func = function foo() {
         print(typeof this, this);
          print(arguments.length);
for (var i = 0; i < arguments.length; i++) {</pre>
              print(i, typeof arguments[i], arguments[i]);
    };
     for (var i = 0;-i < 100; i++) {
func = func.bind('this-' + i, 'arg-' + i);
     print(func.name);
     func();
     test();
} catch (e) {
```

## vulnerability description:

Poc will cause stack overflow. As shown below:

```
ASAN:SIGSEGV
==16827==ERROR: AddressSanitizer: stack-overflow on address 0x7ffeec639ff8 (pc 0x000000041eceb bp 0x7ffeec63a000 sp 0x7ffeec639fe0 T0)
#0 0x41ecea in jsG_markproperty /home/node/xmujs/jsgc.c:76
     #1 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#2 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #3 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #4 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #5 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#6 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #7 0x41efaf in isG markproperty /home/node/xmuis/isgc.c:83
     #8 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#9 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #10 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#11 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #12 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #13 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #14 0x41f19b in isG markobiect /home/node/xmuis/isgc.c:94
     #15 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#16 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #17 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #18 0x41f19b in isG markobiect /home/node/xmuis/isgc.c:94
     #19 0x4lefaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #20 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #21 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#22 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #23 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#24 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #25 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #26 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#27 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #28 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #29 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#30 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #31 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #32 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#33 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #34 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#35 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #36 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #37 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#38 0x41f19b in jsG_markproperty /home/node/xmujs/jsgc.c:94
     #39 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #40 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #41 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78 #42 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94 #43 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #44 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
```

```
#45 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#46 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
#47 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#48 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#49 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78 #50 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#51 0x41efaf in isG markproperty /home/node/xmuis/isgc.c:83
#52 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#53 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
#54 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94 #55 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#56 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#57 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
#58 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#59 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#60 0x41ed74 in jsG markproperty /home/node/xmujs/jsgc.c:77
#61 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#62 0x41f19h in isG markohiect /home/node/xmuis/isgc.c:94
#63 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#64 0x41ed74 in jsG markproperty /home/node/xmujs/jsgc.c:77
#65 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#66 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#67 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #68 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#69 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78 #70 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#71 0x41efaf in jsG markproperty /home/node/xmujs/jsgc.c:83
#72 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#73 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#74 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#75 0x41efaf in jsG markproperty /home/node/xmujs/jsgc.c:83
#76 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#77 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#78 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#79 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#80 0x41ed74 in jsG markproperty /home/node/xmujs/jsgc.c:77
#81 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#82 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
#83 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#84 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#85 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#86 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
#87 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #88 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#89 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78 #90 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#91 0x41efaf in isG markproperty /home/node/xmuis/isgc.c:83
#92 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#93 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
#94 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#95 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#96 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#97 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
#98 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#99 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#100 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77 #101 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#102 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#103 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#104 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#105 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#106 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#107 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #108 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#109 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#110 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#111 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#112 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#113 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#114 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#115 0x41efaf in isG markproperty /home/node/xmuis/isgc.c:83
#116 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#117 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#118 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#119 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#120 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#121 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#122 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#123 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#124 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#125 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#126 0x41f19b in isG markobiect /home/node/xmuis/isgc.c:94
#127 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#128 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#129 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#130 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#131 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#132 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#133 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#134 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#135 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#136 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#137 0x41edf3 in isG markproperty /home/node/xmuis/isgc.c:78
#138 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#139 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#140 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#141 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#142 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#143 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#144 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#145 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#146 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#147 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #148 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#149 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#150 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#151 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#152 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#153 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#154 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#155 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#156 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#157 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
```

```
#158 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #159 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #160 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77 #161 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #162 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#163 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #164 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#165 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #166 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
     #167 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #168 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #169 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #170 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
     #171 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#172 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #173 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
     #174 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #175 0x41efaf in jsG markproperty /home/node/xmujs/jsgc.c:83
     #176 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #177 0x41edf3 in jsG markproperty /home/node/xmujs/jsgc.c:78
     #178 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#179 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #180 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77 #181 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #182 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#183 0x4lefaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #184 0x41ed74 in jsG markproperty /home/node/xmujs/jsgc.c:77
     #185 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #186 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
     #187 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #188 0x41ed74 in jsG markproperty /home/node/xmujs/jsgc.c:77
     #189 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78 #190 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #191 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#192 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #193 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#194 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #195 0x41efaf in jsG markproperty /home/node/xmujs/jsgc.c:83
     #196 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#197 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #198 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#199 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #200 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#201 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #202 0x41f19b in jsG_markobject/home/node/xmujs/jsgc.c:94 #203 0x41efaf in jsG_markproperty/home/node/xmujs/jsgc.c:83
     #204 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#205 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #206 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
     #207 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #208 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #209 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #210 0x41f19b in jsG markobject /home/node/xmujs/jsgc.c:94
     #211 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #212 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #213 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#214 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #215 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #216 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #217 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#218 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #219 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #220 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#221 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #222 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #223 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #224 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #225 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #226 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#227 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #228 0x41ed74 in isG markproperty /home/node/xmuis/isgc.c:77
     #229 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #230 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #231 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83 #232 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #233 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #234 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #235 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #236 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #237 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #238 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #239 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #240 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #241 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #242 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#243 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #244 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77 #245 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #246 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #247 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
     #248 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
     #249 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
     #250 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
     #251 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
SUMMARY: AddressSanitizer: stack-overflow /home/node/xmujs/jsgc.c:76 jsG_markproperty
```

rain6851 commented on May 7, 2020

@ccxvii @sebras please check the issues.

Author

We are aware of the issues. We will get around to them when we have time. If you need a fix more urgently than that, you're more than welcome to submit a patch.

rain6851 commented on May 8, 2020

We are aware of the issues. We will get around to them when we have time. If you need a fix more urgently than that, you're more than welcome to submit a patch.

Ok!

Coxvii commented on May 27, 2020

Coxvii commented on May 27, 2020

This should be fixed in the following commit. Thanks for the report!

commit 331c5ec

Author: Tor Andersson@artifex.com

Date: Thu May 14 13:42:00 2020 +0200

Issue 133: Eliminate recursion in 6C scanning phase.

Use a queue instead of recursion to scan reachable objects.

ccxvii closed this as completed on May 27, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone
Development
No branches or pull requests

2 participants

