stack overflow #134

Closed **rain6851** opened this issue on Apr 17, 2020 · 3 comments

rain6851 commented on Apr 17, 2020

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-67
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;

    // 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('F()', F.name);
    F();
    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 Math.max()
    // if DUK_USE_LIGHTFUNC_BUILTINS is enabled.

    // Long chain.

    func = function foo() {
        print(typeof this, this);
        print(arguments.length);
        for (var i = 0; i < arguments.length; i++) {
            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();
}

try {
    test();
} catch (e) {
}
```

vulnerability description:

Poc will cause stack overflow. As shown below:

```
ASAN:SIGSEGV
=================================================================
==19628==ERROR: AddressSanitizer: stack-overflow on address 0x7ffd0fa89ff8 (pc 0x00000041ecf2 bp 0x7ffd0fa8a010 sp 0x7ffd0fa89ff0 T0)
    #0 0x41ecf1 in jsG_markproperty /home/node/xmujs/jsgc.c:76
    #1 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #2 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #3 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #4 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #5 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #6 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #7 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #8 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #9 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #10 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #11 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #12 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #13 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #14 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #15 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #16 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #17 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #18 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #19 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #20 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #21 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #22 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #23 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #24 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #25 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #26 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #27 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #28 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #29 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #30 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #31 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #32 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #33 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #34 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #35 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #36 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #37 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #38 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #39 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #40 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #41 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #42 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #43 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
```

```
#44 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#45 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#46 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#47 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#48 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#49 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#50 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#51 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#52 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#53 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#54 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#55 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#56 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#57 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#58 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#59 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#60 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#61 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#62 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#63 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#64 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#65 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#66 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#67 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#68 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#69 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#70 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#71 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#72 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#73 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#74 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#75 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#76 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#77 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#78 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#79 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#80 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#81 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#82 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#83 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#84 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#85 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#86 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#87 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#88 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#89 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#90 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#91 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#92 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#93 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#94 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#95 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#96 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#97 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#98 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#99 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#100 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#101 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#102 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#103 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#104 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#105 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#106 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#107 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#108 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#109 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#110 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#111 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#112 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#113 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#114 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#115 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#116 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#117 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#118 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#119 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#120 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#121 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#122 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#123 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#124 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#125 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#126 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#127 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#128 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#129 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#130 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#131 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#132 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#133 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#134 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#135 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#136 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#137 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#138 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#139 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#140 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#141 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#142 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#143 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#144 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#145 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#146 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#147 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#148 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#149 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#150 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#151 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#152 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
#153 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
#154 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
#155 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
#156 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
```

```
    #157 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #158 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #159 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #160 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #161 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #162 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #163 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #164 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #165 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #166 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #167 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #168 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #169 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #170 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #171 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #172 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #173 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #174 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #175 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #176 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #177 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #178 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #179 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #180 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #181 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #182 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #183 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #184 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #185 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #186 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #187 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #188 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #189 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #190 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #191 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #192 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #193 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #194 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #195 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #196 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #197 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #198 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #199 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #200 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #201 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #202 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #203 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #204 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #205 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #206 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #207 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #208 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #209 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #210 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #211 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #212 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #213 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #214 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #215 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #216 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #217 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #218 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #219 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #220 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #221 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #222 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #223 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #224 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #225 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #226 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #227 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #228 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #229 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #230 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #231 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #232 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #233 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #234 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #235 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #236 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #237 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #238 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #239 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #240 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #241 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #242 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #243 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #244 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #245 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #246 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #247 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78
    #248 0x41f19b in jsG_markobject /home/node/xmujs/jsgc.c:94
    #249 0x41efaf in jsG_markproperty /home/node/xmujs/jsgc.c:83
    #250 0x41ed74 in jsG_markproperty /home/node/xmujs/jsgc.c:77
    #251 0x41edf3 in jsG_markproperty /home/node/xmujs/jsgc.c:78

SUMMARY: AddressSanitizer: stack-overflow /home/node/xmujs/jsgc.c:76 jsG_markproperty
==19628==ABORTING
```

rain6851 commented on May 7, 2020 — Author

@ccxvii **@sebras** please check the issues.

yurivict commented on May 10, 2020

Reproducible on FreeBSD:

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==18375==ERROR: AddressSanitizer: stack-overflow on address 0x7fffdfffffe8 (pc 0x0000002f218a bp 0x7fffe0000150 sp 0x7fffdfffffe0 T0)
    #0 0x2f2189 in jsG_markobject /usr/ports/lang/mujs/work/mujs-1.0.7/./jsgc.c:94:34

SUMMARY: AddressSanitizer: stack-overflow /usr/ports/lang/mujs/work/mujs-1.0.7/./jsgc.c:94:34 in jsG_markobject
==18375==ABORTING
```

ccxvii commented on May 27, 2020 Owner

Should be fixed with the same commit that fixed issue 133. Thanks for the report!

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

3 participants