New issue

Jump to bottom

A stack overflow in q.c:1147 causes Segmentation fault #141

Open seviezhou opened this issue on Aug 7, 2020 · 0 comments

seviezhou commented on Aug 7, 2020

System info

Ubuntu x86_64, clang 6.0, swfdump (latest master fad6c2)

Command line

./src/swfdump -D @@

Output

```
[stack:98 locals:0 scope:12-0 flags: need_rest has_optional has_param_names] slot:0
<metadata>final override  function * NULL=()(0 params, 0 optional)
[stack:98 locals:0 scope:12-0 flags: need_rest has_optional has_param_names] slot:0
<metadata>final override  function * NULL=()(0 params, 0 optional)
[stack:98 locals:0 scope:12-0 flags: need_rest has_optional has_param_names] slot:0
<metadata>final override  function * NULL=()(0 params, 0 optional)
[stack:98 locals:0 scope:12-0 flags: need_rest has_optional has_param_names] slot:0
<metadata>final override  function * NULL=()(0 params, 0 optional)
[stack:98 locals:0 scope:12-0 flags: need_rest has_optional has_param_names] slot:0
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==61651==ERROR: AddressSanitizer: stack-overflow on address 0x7ffed2a2cff8 (pc 0x7f0e233a17cc bp 0x7ffed2a2d910 sp 0x7ffed2a2d000 T0)
    #0 0x7f0e233a17cb  (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x227cb)
    #1 0x7f0e234175e2 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x985e2)
    #2 0x560bfedb6ca7 in rfx_alloc /home/seviezhou/swftools/lib/mem.c:30
    #3 0x560bfeda2885 in dict_put /home/seviezhou/swftools/lib/q.c:1147
    #4 0x560bfecf6d18 in dump_method as3/abc.c:358
    #5 0x560bfecf829a in traits_dump as3/abc.c:596
    #6 0x560bfecf765a in dump_method as3/abc.c:403
    #7 0x560bfecf829a in traits_dump as3/abc.c:596
    #8 0x560bfecf765a in dump_method as3/abc.c:403
    #9 0x560bfecf829a in traits_dump as3/abc.c:596
    #10 0x560bfecf765a in dump_method as3/abc.c:403
    #11 0x560bfecf829a in traits_dump as3/abc.c:596
    #12 0x560bfecf765a in dump_method as3/abc.c:403
    #13 0x560bfecf829a in traits_dump as3/abc.c:596
    #14 0x560bfecf765a in dump_method as3/abc.c:403
    #15 0x560bfecf829a in traits_dump as3/abc.c:596
    #16 0x560bfecf765a in dump_method as3/abc.c:403
    #17 0x560bfecf829a in traits_dump as3/abc.c:596
    #18 0x560bfecf765a in dump_method as3/abc.c:403
    #19 0x560bfecf829a in traits_dump as3/abc.c:596
    #20 0x560bfecf765a in dump_method as3/abc.c:403
    #21 0x560bfecf829a in traits_dump as3/abc.c:596
    #22 0x560bfecf765a in dump_method as3/abc.c:403
    #23 0x560bfecf829a in traits_dump as3/abc.c:596
    #24 0x560bfecf765a in dump_method as3/abc.c:403
    #25 0x560bfecf829a in traits_dump as3/abc.c:596
    #26 0x560bfecf765a in dump_method as3/abc.c:403
    #27 0x560bfecf829a in traits_dump as3/abc.c:596
    #28 0x560bfecf765a in dump_method as3/abc.c:403
    #29 0x560bfecf829a in traits_dump as3/abc.c:596
    #30 0x560bfecf765a in dump_method as3/abc.c:403
    #31 0x560bfecf829a in traits_dump as3/abc.c:596
    #32 0x560bfecf765a in dump_method as3/abc.c:403
    #33 0x560bfecf829a in traits_dump as3/abc.c:596
    #34 0x560bfecf765a in dump_method as3/abc.c:403
    #35 0x560bfecf829a in traits_dump as3/abc.c:596
    #36 0x560bfecf765a in dump_method as3/abc.c:403
    #37 0x560bfecf829a in traits_dump as3/abc.c:596
    #38 0x560bfecf765a in dump_method as3/abc.c:403
    #39 0x560bfecf829a in traits_dump as3/abc.c:596
    #40 0x560bfecf765a in dump_method as3/abc.c:403
    #41 0x560bfecf829a in traits_dump as3/abc.c:596
    #42 0x560bfecf765a in dump_method as3/abc.c:403
    #43 0x560bfecf829a in traits_dump as3/abc.c:596
    #44 0x560bfecf765a in dump_method as3/abc.c:403
    #45 0x560bfecf829a in traits_dump as3/abc.c:596
    #46 0x560bfecf765a in dump_method as3/abc.c:403
    #47 0x560bfecf829a in traits_dump as3/abc.c:596
    #48 0x560bfecf765a in dump_method as3/abc.c:403
    #49 0x560bfecf829a in traits_dump as3/abc.c:596
    #50 0x560bfecf765a in dump_method as3/abc.c:403
    #51 0x560bfecf829a in traits_dump as3/abc.c:596
    #52 0x560bfecf765a in dump_method as3/abc.c:403
    #53 0x560bfecf829a in traits_dump as3/abc.c:596
    #54 0x560bfecf765a in dump_method as3/abc.c:403
    #55 0x560bfecf829a in traits_dump as3/abc.c:596
    #56 0x560bfecf765a in dump_method as3/abc.c:403
    #57 0x560bfecf829a in traits_dump as3/abc.c:596
    #58 0x560bfecf765a in dump_method as3/abc.c:403
```

```
#59 0x560bfecf829a in traits_dump as3/abc.c:596
#60 0x560bfecf765a in dump_method as3/abc.c:403
#61 0x560bfecf829a in traits_dump as3/abc.c:596
#62 0x560bfecf765a in dump_method as3/abc.c:403
#63 0x560bfecf829a in traits_dump as3/abc.c:596
#64 0x560bfecf765a in dump_method as3/abc.c:403
#65 0x560bfecf829a in traits_dump as3/abc.c:596
#66 0x560bfecf765a in dump_method as3/abc.c:403
#67 0x560bfecf829a in traits_dump as3/abc.c:596
#68 0x560bfecf765a in dump_method as3/abc.c:403
#69 0x560bfecf829a in traits_dump as3/abc.c:596
#70 0x560bfecf765a in dump_method as3/abc.c:403
#71 0x560bfecf829a in traits_dump as3/abc.c:596
#72 0x560bfecf765a in dump_method as3/abc.c:403
#73 0x560bfecf829a in traits_dump as3/abc.c:596
#74 0x560bfecf765a in dump_method as3/abc.c:403
#75 0x560bfecf829a in traits_dump as3/abc.c:596
#76 0x560bfecf765a in dump_method as3/abc.c:403
#77 0x560bfecf829a in traits_dump as3/abc.c:596
#78 0x560bfecf765a in dump_method as3/abc.c:403
#79 0x560bfecf829a in traits_dump as3/abc.c:596
#80 0x560bfecf765a in dump_method as3/abc.c:403
#81 0x560bfecf829a in traits_dump as3/abc.c:596
#82 0x560bfecf765a in dump_method as3/abc.c:403
#83 0x560bfecf829a in traits_dump as3/abc.c:596
#84 0x560bfecf765a in dump_method as3/abc.c:403
#85 0x560bfecf829a in traits_dump as3/abc.c:596
#86 0x560bfecf765a in dump_method as3/abc.c:403
#87 0x560bfecf829a in traits_dump as3/abc.c:596
#88 0x560bfecf765a in dump_method as3/abc.c:403
#89 0x560bfecf829a in traits_dump as3/abc.c:596
#90 0x560bfecf765a in dump_method as3/abc.c:403
#91 0x560bfecf829a in traits_dump as3/abc.c:596
#92 0x560bfecf765a in dump_method as3/abc.c:403
#93 0x560bfecf829a in traits_dump as3/abc.c:596
#94 0x560bfecf765a in dump_method as3/abc.c:403
#95 0x560bfecf829a in traits_dump as3/abc.c:596
#96 0x560bfecf765a in dump_method as3/abc.c:403
#97 0x560bfecf829a in traits_dump as3/abc.c:596
#98 0x560bfecf765a in dump_method as3/abc.c:403
#99 0x560bfecf829a in traits_dump as3/abc.c:596
#100 0x560bfecf765a in dump_method as3/abc.c:403
#101 0x560bfecf829a in traits_dump as3/abc.c:596
#102 0x560bfecf765a in dump_method as3/abc.c:403
#103 0x560bfecf829a in traits_dump as3/abc.c:596
#104 0x560bfecf765a in dump_method as3/abc.c:403
#105 0x560bfecf829a in traits_dump as3/abc.c:596
#106 0x560bfecf765a in dump_method as3/abc.c:403
#107 0x560bfecf829a in traits_dump as3/abc.c:596
#108 0x560bfecf765a in dump_method as3/abc.c:403
#109 0x560bfecf829a in traits_dump as3/abc.c:596
#110 0x560bfecf765a in dump_method as3/abc.c:403
#111 0x560bfecf829a in traits_dump as3/abc.c:596
#112 0x560bfecf765a in dump_method as3/abc.c:403
#113 0x560bfecf829a in traits_dump as3/abc.c:596
#114 0x560bfecf765a in dump_method as3/abc.c:403
#115 0x560bfecf829a in traits_dump as3/abc.c:596
#116 0x560bfecf765a in dump_method as3/abc.c:403
#117 0x560bfecf829a in traits_dump as3/abc.c:596
#118 0x560bfecf765a in dump_method as3/abc.c:403
#119 0x560bfecf829a in traits_dump as3/abc.c:596
#120 0x560bfecf765a in dump_method as3/abc.c:403
#121 0x560bfecf829a in traits_dump as3/abc.c:596
#122 0x560bfecf765a in dump_method as3/abc.c:403
#123 0x560bfecf829a in traits_dump as3/abc.c:596
#124 0x560bfecf765a in dump_method as3/abc.c:403
#125 0x560bfecf829a in traits_dump as3/abc.c:596
#126 0x560bfecf765a in dump_method as3/abc.c:403
#127 0x560bfecf829a in traits_dump as3/abc.c:596
#128 0x560bfecf765a in dump_method as3/abc.c:403
#129 0x560bfecf829a in traits_dump as3/abc.c:596
#130 0x560bfecf765a in dump_method as3/abc.c:403
#131 0x560bfecf829a in traits_dump as3/abc.c:596
#132 0x560bfecf765a in dump_method as3/abc.c:403
#133 0x560bfecf829a in traits_dump as3/abc.c:596
#134 0x560bfecf765a in dump_method as3/abc.c:403
#135 0x560bfecf829a in traits_dump as3/abc.c:596
#136 0x560bfecf765a in dump_method as3/abc.c:403
#137 0x560bfecf829a in traits_dump as3/abc.c:596
#138 0x560bfecf765a in dump_method as3/abc.c:403
#139 0x560bfecf829a in traits_dump as3/abc.c:596
#140 0x560bfecf765a in dump_method as3/abc.c:403
#141 0x560bfecf829a in traits_dump as3/abc.c:596
#142 0x560bfecf765a in dump_method as3/abc.c:403
#143 0x560bfecf829a in traits_dump as3/abc.c:596
#144 0x560bfecf765a in dump_method as3/abc.c:403
#145 0x560bfecf829a in traits_dump as3/abc.c:596
#146 0x560bfecf765a in dump_method as3/abc.c:403
#147 0x560bfecf829a in traits_dump as3/abc.c:596
#148 0x560bfecf765a in dump_method as3/abc.c:403
#149 0x560bfecf829a in traits_dump as3/abc.c:596
#150 0x560bfecf765a in dump_method as3/abc.c:403
#151 0x560bfecf829a in traits_dump as3/abc.c:596
#152 0x560bfecf765a in dump_method as3/abc.c:403
#153 0x560bfecf829a in traits_dump as3/abc.c:596
#154 0x560bfecf765a in dump_method as3/abc.c:403
#155 0x560bfecf829a in traits_dump as3/abc.c:596
#156 0x560bfecf765a in dump_method as3/abc.c:403
#157 0x560bfecf829a in traits_dump as3/abc.c:596
#158 0x560bfecf765a in dump_method as3/abc.c:403
#159 0x560bfecf829a in traits_dump as3/abc.c:596
#160 0x560bfecf765a in dump_method as3/abc.c:403
#161 0x560bfecf829a in traits_dump as3/abc.c:596
#162 0x560bfecf765a in dump_method as3/abc.c:403
#163 0x560bfecf829a in traits_dump as3/abc.c:596
#164 0x560bfecf765a in dump_method as3/abc.c:403
#165 0x560bfecf829a in traits_dump as3/abc.c:596
#166 0x560bfecf765a in dump_method as3/abc.c:403
#167 0x560bfecf829a in traits_dump as3/abc.c:596
#168 0x560bfecf765a in dump_method as3/abc.c:403
#169 0x560bfecf829a in traits_dump as3/abc.c:596
#170 0x560bfecf765a in dump_method as3/abc.c:403
#171 0x560bfecf829a in traits_dump as3/abc.c:596
```

```
    #172 0x560bfecf765a in dump_method as3/abc.c:403
    #173 0x560bfecf829a in traits_dump as3/abc.c:596
    #174 0x560bfecf765a in dump_method as3/abc.c:403
    #175 0x560bfecf829a in traits_dump as3/abc.c:596
    #176 0x560bfecf765a in dump_method as3/abc.c:403
    #177 0x560bfecf829a in traits_dump as3/abc.c:596
    #178 0x560bfecf765a in dump_method as3/abc.c:403
    #179 0x560bfecf829a in traits_dump as3/abc.c:596
    #180 0x560bfecf765a in dump_method as3/abc.c:403
    #181 0x560bfecf829a in traits_dump as3/abc.c:596
    #182 0x560bfecf765a in dump_method as3/abc.c:403
    #183 0x560bfecf829a in traits_dump as3/abc.c:596
    #184 0x560bfecf765a in dump_method as3/abc.c:403
    #185 0x560bfecf829a in traits_dump as3/abc.c:596
    #186 0x560bfecf765a in dump_method as3/abc.c:403
    #187 0x560bfecf829a in traits_dump as3/abc.c:596
    #188 0x560bfecf765a in dump_method as3/abc.c:403
    #189 0x560bfecf829a in traits_dump as3/abc.c:596
    #190 0x560bfecf765a in dump_method as3/abc.c:403
    #191 0x560bfecf829a in traits_dump as3/abc.c:596
    #192 0x560bfecf765a in dump_method as3/abc.c:403
    #193 0x560bfecf829a in traits_dump as3/abc.c:596
    #194 0x560bfecf765a in dump_method as3/abc.c:403
    #195 0x560bfecf829a in traits_dump as3/abc.c:596
    #196 0x560bfecf765a in dump_method as3/abc.c:403
    #197 0x560bfecf829a in traits_dump as3/abc.c:596
    #198 0x560bfecf765a in dump_method as3/abc.c:403
    #199 0x560bfecf829a in traits_dump as3/abc.c:596
    #200 0x560bfecf765a in dump_method as3/abc.c:403
    #201 0x560bfecf829a in traits_dump as3/abc.c:596
    #202 0x560bfecf765a in dump_method as3/abc.c:403
    #203 0x560bfecf829a in traits_dump as3/abc.c:596
    #204 0x560bfecf765a in dump_method as3/abc.c:403
    #205 0x560bfecf829a in traits_dump as3/abc.c:596
    #206 0x560bfecf765a in dump_method as3/abc.c:403
    #207 0x560bfecf829a in traits_dump as3/abc.c:596
    #208 0x560bfecf765a in dump_method as3/abc.c:403
    #209 0x560bfecf829a in traits_dump as3/abc.c:596
    #210 0x560bfecf765a in dump_method as3/abc.c:403
    #211 0x560bfecf829a in traits_dump as3/abc.c:596
    #212 0x560bfecf765a in dump_method as3/abc.c:403
    #213 0x560bfecf829a in traits_dump as3/abc.c:596
    #214 0x560bfecf765a in dump_method as3/abc.c:403
    #215 0x560bfecf829a in traits_dump as3/abc.c:596
    #216 0x560bfecf765a in dump_method as3/abc.c:403
    #217 0x560bfecf829a in traits_dump as3/abc.c:596
    #218 0x560bfecf765a in dump_method as3/abc.c:403
    #219 0x560bfecf829a in traits_dump as3/abc.c:596
    #220 0x560bfecf765a in dump_method as3/abc.c:403
    #221 0x560bfecf829a in traits_dump as3/abc.c:596
    #222 0x560bfecf765a in dump_method as3/abc.c:403
    #223 0x560bfecf829a in traits_dump as3/abc.c:596
    #224 0x560bfecf765a in dump_method as3/abc.c:403
    #225 0x560bfecf829a in traits_dump as3/abc.c:596
    #226 0x560bfecf765a in dump_method as3/abc.c:403
    #227 0x560bfecf829a in traits_dump as3/abc.c:596
    #228 0x560bfecf765a in dump_method as3/abc.c:403
    #229 0x560bfecf829a in traits_dump as3/abc.c:596
    #230 0x560bfecf765a in dump_method as3/abc.c:403
    #231 0x560bfecf829a in traits_dump as3/abc.c:596
    #232 0x560bfecf765a in dump_method as3/abc.c:403
    #233 0x560bfecf829a in traits_dump as3/abc.c:596
    #234 0x560bfecf765a in dump_method as3/abc.c:403
    #235 0x560bfecf829a in traits_dump as3/abc.c:596
    #236 0x560bfecf765a in dump_method as3/abc.c:403
    #237 0x560bfecf829a in traits_dump as3/abc.c:596
    #238 0x560bfecf765a in dump_method as3/abc.c:403
    #239 0x560bfecf829a in traits_dump as3/abc.c:596
    #240 0x560bfecf765a in dump_method as3/abc.c:403
    #241 0x560bfecf829a in traits_dump as3/abc.c:596
    #242 0x560bfecf765a in dump_method as3/abc.c:403
    #243 0x560bfecf829a in traits_dump as3/abc.c:596
    #244 0x560bfecf765a in dump_method as3/abc.c:403
    #245 0x560bfecf829a in traits_dump as3/abc.c:596
    #246 0x560bfecf765a in dump_method as3/abc.c:403
    #247 0x560bfecf829a in traits_dump as3/abc.c:596
    #248 0x560bfecf765a in dump_method as3/abc.c:403
    #249 0x560bfecf829a in traits_dump as3/abc.c:596
    #250 0x560bfecf765a in dump_method as3/abc.c:403
    #251 0x560bfecf829a in traits_dump as3/abc.c:596

SUMMARY: AddressSanitizer: stack-overflow ??:0 ??
==61651==ABORTING
```

POC

stack-overflow-dict_put-q-1147.zip

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant