New issue

Jump to bottom

A heap-buffer-overflow in q.c:727 #125

Open seviezhou opened this issue on Aug 5, 2020 · 0 comments

seviezhou commented on Aug 5, 2020

System info

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

Command line

./src/swfdump -D @@

AddressSanitizer output

```
=================================================================
==50415==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000efc2 at pc 0x55885e14b03a bp 0x7fff88438ab0 sp 0x7fff88438aa0
READ of size 1 at 0x60300000efc2 thread T0
    #0 0x55885e14b039 in string_hash /home/seviezhou/swftools/lib/q.c:727
    #1 0x55885e14e879 in dict_put /home/seviezhou/swftools/lib/q.c:1146
    #2 0x55885e15486b in array_append /home/seviezhou/swftools/lib/q.c:1531
    #3 0x55885e0c2c7d in pool_read as3/pool.c:1130
    #4 0x55885e0aef44 in swf_ReadABC as3/abc.c:748
    #5 0x55885e024003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #6 0x7fde3d2e9b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x55885e027439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

0x60300000efc2 is located 0 bytes to the right of 18-byte region [0x60300000efb0,0x60300000efc2)
allocated by thread T0 here:
    #0 0x7fde3d96e612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
    #1 0x55885e162ca7 in rfx_alloc /home/seviezhou/swftools/lib/mem.c:30
    #2 0x55885e171096  (/home/seviezhou/swftools/src/swfdump+0x21a096)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/swftools/lib/q.c:727 string_hash
Shadow bytes around the buggy address:
  0x0c067fff9da0: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
  0x0c067fff9db0: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
  0x0c067fff9dc0: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x0c067fff9dd0: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
  0x0c067fff9de0: 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa
=>0x0c067fff9df0: fd fd fd fd fa fa 00 00[02]fa fa fa 00 00 02 fa
  0x0c067fff9e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9e20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c067fff9e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
==50415==ABORTING
```

POC

heap-overflow-string_hash-q-727.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