New issue

Jump to bottom

A heap-buffer-overflow in rfxswf.c:520 #124

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

```
/home/seviezhou/swftools/lib/rfxswf.c:520
    #1 0x55e4357ac829 in pool_read as3/pool.c:1119
    #2 0x55e435798f44 in swf_ReadABC as3/abc.c:748
    #3 0x55e43570e003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #4 0x7f3431472b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55e435711439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

0x60400000df7b is located 0 bytes to the right of 43-byte region [0x60400000df50,0x60400000df7b)
allocated by thread T0 here:
    #0 0x7f3431af7612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
    #1 0x55e43584cca7 in rfx_alloc /home/seviezhou/swftools/lib/mem.c:30
    #2 0x55e43585b096  (/home/seviezhou/swftools/src/swfdump+0x21a096)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/swftools/lib/rfxswf.c:520 swf_GetD64
Shadow bytes around the buggy address:
  0x0c087fff9b90: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff9ba0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff9bb0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff9bc0: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c087fff9bd0: fa fa 00 00 00 00 00 05 fa fa 00 00 00 00 05 fa
=>0x0c087fff9be0: fa fa 00 00 00 00 00 07 fa fa 00 00 00 00 00[03]
  0x0c087fff9bf0: fa fa 00 00 00 00 03 fa fa fa 00 00 00 00 05 fa
  0x0c087fff9c00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff9c10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff9c20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c087fff9c30: 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
==29380==ABORTING
```

POC

heap-overflow-swf_GetD64-rfxswf-520.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