New issue

Jump to bottom

A heap-buffer-overflow in swfobject.c:195 #122

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

```
=================================================================
==16659==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000ef95 at pc 0x7f6f9085a1fb bp 0x7ffd450e1b90 sp 0x7ffd450e1338
READ of size 1 at 0x60200000ef95 thread T0
    #0 0x7f6f9085a1fa in strlen (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x701fa)
    #1 0x564d72dccc05 in swf_GetPlaceObject modules/swfobject.c:195
    #2 0x564d72da4174 in main /home/seviezhou/swftools/src/swfdump.c:1341
    #3 0x7f6f901fdb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #4 0x564d72da8439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

0x60200000ef95 is located 0 bytes to the right of 5-byte region [0x60200000ef90,0x60200000ef95)
allocated by thread T0 here:
    #0 0x7f6f90882612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
    #1 0x564d72ee3ca7 in rfx_alloc /home/seviezhou/swftools/lib/mem.c:30
    #2 0x564d72ef2096  (/home/seviezhou/swftools/src/swfdump+0x21a096)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 strlen
Shadow bytes around the buggy address:
  0x0c047fff9da0: fa fa fd fd fa fa fd fa fa fa fd fd fa fa 06 fa
  0x0c047fff9db0: fa fa 00 00 fa fa 06 fa fa fa 00 00 fa fa 06 fa
  0x0c047fff9dc0: fa fa 00 00 fa fa 06 fa fa fa 00 00 fa fa 06 fa
  0x0c047fff9dd0: fa fa 00 00 fa fa 06 fa fa fa 00 00 fa fa fd fa
  0x0c047fff9de0: fa fa 00 00 fa fa 00 fa fa fa 05 fa fa fa 00 01
=>0x0c047fff9df0: fa fa[05]fa fa fa 00 06 fa fa 04 fa fa fa 03 fa
  0x0c047fff9e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9e20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff9e40: 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
==16659==ABORTING
```

POC

heap-overflow-swf_GetPlaceObject-swfobject-195.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