

New issue

Jump to bottom

# A heap-buffer-overflow in swfdump.c:1406 #121

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

```
=====
==46368==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000ef52 at pc 0x7f3ab3fed1fb bp 0x7ffd0e92b0f0 sp 0x7ffd0e92a898
READ of size 3 at 0x6020000ef52 thread T0
#0 0x7f3ab3fed1fa in strlen (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x701fa)
#1 0x55b50c3223a4 in main /home/seviezhou/swftools/src/swfdump.c:1406
#2 0x7f3ab3990b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#3 0x55b50c325439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

0x6020000ef52 is located 0 bytes to the right of 2-byte region [0x6020000ef50,0x6020000ef52)
allocated by thread T0 here:
#0 0x7f3ab4015612 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98612)
#1 0x55b50c460ca7 in rfx_alloc /home/seviezhou/swftools/lib/mem.c:30
#2 0x55b50c46f096 (/home/seviezhou/swftools/src/swfdump+0x21a096)

SUMMARY: AddressSanitizer: heap-buffer-overflow ??:0 strlen
Shadow bytes around the buggy address:
 0x0c047fff9d90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9da0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9db0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9dc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c047fff9dd0: fa fa fa fa fa fa fa fa fa fa 01 fa fa 01 fa
=>0x0c047fff9de0: fa 01 fa fa 00 02 fa fa[02]fa fa 01 fa
0x0c047fff9df0: fa 01 fa fa 05 fa fa 00 02 fa fa 00 04
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
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
==46368==ABORTING
```

## POC

heap-overflow-main-swfdump-1406.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

