New issue

Jump to bottom

A Segmentation fault in swfaction.c:483 #115

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

seviezhou commented on Aug 5, 2020 • edited

System info

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

Command line

./src/swfdump -D @@

Output

```
Segmentation fault (core dumped)
```

AddressSanitizer output

```
ASAN:SIGSEGV
=================================================================
==15645==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7fed57f575c7 bp 0x7ffcbf871410 sp 0x7ffcbf870e98 T0)
    #0 0x7fed57f575c6  (/lib/x86_64-linux-gnu/libc.so.6+0x18e5c6)
    #1 0x7fed57e264d2 in vfprintf (/lib/x86_64-linux-gnu/libc.so.6+0x5d4d2)
    #2 0x7fed57efb2eb in __printf_chk (/lib/x86_64-linux-gnu/libc.so.6+0x1322eb)
    #3 0x55e63636c9fb in printf /usr/include/x86_64-linux-gnu/bits/stdio2.h:104
    #4 0x55e63636c9fb in swf_DumpActions modules/swfaction.c:483
    #5 0x55e6363586bd in main /home/seviezhou/swftools/src/swfdump.c:1585
    #6 0x7fed57deab96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x55e63635c439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
==15645==ABORTING
```

POC

SEGV-swf_DumpActions-swfaction-483.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