New issue

Jump to bottom

A Segmentation fault in abc.c:625 #129

Open seviezhou opened this issue on Aug 6, 2020 · 0 comments

seviezhou commented on Aug 6, 2020

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
=================================================================
==55887==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x5608561c25bc bp 0x5608562873e0 sp 0x7ffd9e332360 T0)
    #0 0x5608561c25bb in swf_DumpABC as3/abc.c:625
    #1 0x560856139038 in main /home/seviezhou/swftools/src/swfdump.c:1578
    #2 0x7f84a4ac5b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #3 0x56085613c439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/abc.c:625 swf_DumpABC
==55887==ABORTING
```

POC

SEGV-swf_DumpABC-abc-625.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