New issue

Jump to bottom

A Segmentation fault in abc.c:58 #137

○ 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
=================================================================
==65202==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f4e7a0295a1 bp 0x000000000000 sp 0x7ffeec6b0328 T0)
    #0 0x7f4e7a0295a0  (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0)
    #1 0x7f4e79f1a204 in fputs (/lib/x86_64-linux-gnu/libc.so.6+0x7f204)
    #2 0x555f109567ea in fprintf /usr/include/x86_64-linux-gnu/bits/stdio2.h:97
    #3 0x555f109567ea in params_dump as3/abc.c:58
    #4 0x555f109567ea in dump_method as3/abc.c:369
    #5 0x555f10961433 in swf_DumpABC as3/abc.c:722
    #6 0x555f108d7038 in main /home/seviezhou/swftools/src/swfdump.c:1578
    #7 0x7f4e79ebcb96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x555f108da439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
==65202==ABORTING
```

POC

SEGV-params_dump-abc-58.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