<> Code   ⊙ Issues 118   ⭒ Pull requests 5   ▶ Actions   ⊞ Projects   📖 Wiki   •••

New issue   Jump to bottom

A Segmentation fault in abc.c:602 #133

⊙ 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
=================================================================
==31886==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x55d8b550d4f4 bp 0x60200000e6f0 sp 0x7ffe6a230970 T0)
    #0 0x55d8b550d4f3 in traits_dump as3/abc.c:602
    #1 0x55d8b5516ebc in swf_DumpABC as3/abc.c:689
    #2 0x55d8b548d038 in main /home/seviezhou/swftools/src/swfdump.c:1578
    #3 0x7f8c5b793b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #4 0x55d8b5490439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/abc.c:602 traits_dump
==31886==ABORTING
```

POC

SEGV-traits_dump-abc-602.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