New issue

Jump to bottom

A Segmentation fault in code.c:982 #143

Open seviezhou opened this issue on Aug 7, 2020 · 0 comments

seviezhou commented on Aug 7, 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
=================================================================
==22794==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000018 (pc 0x55ca6dccf468 bp 0x000000000000 sp 0x7ffcc4b1cd30 T0)
    #0 0x55ca6dccf467 in code_dump2 as3/code.c:982
    #1 0x55ca6dc986bf in dump_method as3/abc.c:405
    #2 0x55ca6dca3433 in swf_DumpABC as3/abc.c:722
    #3 0x55ca6dc19038 in main /home/seviezhou/swftools/src/swfdump.c:1578
    #4 0x7f1480cd1b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55ca6dc1c439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/code.c:982 code_dump2
==22794==ABORTING
```

POC

SEGV-code_dump2-code-982.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