matthiaskramm / swftools Public

Code Issues 118 Pull requests 5 Actions Projects Wiki ···

New issue

Jump to bottom

A Segmentation fault in code.c:754 #145

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
=================================================================
==9224==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000028 (pc 0x559475594d38 bp 0x000000000000 sp 0x7fffe52943c0 T0)
    #0 0x559475594d37 in callcode as3/code.c:754
    #1 0x55947559dffe in code_get_stats as3/code.c:885
    #2 0x55947559e8ef in code_dump2 as3/code.c:921
    #3 0x5594755686bf in dump_method as3/abc.c:405
    #4 0x559475573433 in swf_DumpABC as3/abc.c:722
    #5 0x5594754e9038 in main /home/seviezhou/swftools/src/swfdump.c:1578
    #6 0x7f5b9fce3b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x5594754ec439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/code.c:754 callcode
==9224==ABORTING
```

POC

SEGV-callcode-code-754.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