


New issue

Jump to bottom

A Segmentation fault in abc.c:361 #128

 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
=====
==35749==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55e82ff9dda0 bp 0x55e83006d140 sp 0x7ffdfc2bfc80 T0)
#0 0x55e82ff9dd9f in dump_method as3/abc.c:361
#1 0x55e82ffa91a4 in swf_DumpABC as3/abc.c:707
#2 0x55e82ff1f038 in main /home/seviezhou/swftools/src/swfdump.c:1578
#3 0x7f6a32462b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
#4 0x55e82ff22439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/abc.c:361 dump_method
==35749==ABORTING
```

POC

[SEGV-dump_method-abc-361.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

