New issue

Jump to bottom

A Segmentation fault in code.c:357 #146

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
=================================================================
==80352==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f3928a955a1 bp 0x7ffc790bda50 sp 0x7ffc790bd1d8 T0)
    #0 0x7f3928a955a0  (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0)
    #1 0x7f3928f771a8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8)
    #2 0x55cb3f1d0417 in code_parse as3/code.c:357
    #3 0x55cb3f1ad810 in swf_ReadABC as3/abc.c:877
    #4 0x55cb3f121003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #5 0x7f3928928b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #6 0x55cb3f124439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ??:0 ??
==80352==ABORTING
```

POC

SEGV-code_parse-code-357.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