New issue

Jump to bottom

# A Segmentation fault in swftext.c:225 #139

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
=================================================================
==75376==ERROR: AddressSanitizer: SEGV on unknown address 0x61900004697c (pc 0x560559a71dfc bp 0x000000008c00 sp 0x7ffde49444e0 T0)
    #0 0x560559a71dfb in swf_FontExtract_DefineFontInfo modules/swftext.c:225
    #1 0x560559a773e6 in swf_FontExtract modules/swftext.c:611
    #2 0x560559a385dc in fontcallback2 /home/seviezhou/swftools/src/swfdump.c:941
    #3 0x560559a70920 in swf_FontEnumerate modules/swftext.c:133
    #4 0x560559a35273 in main /home/seviezhou/swftools/src/swfdump.c:1296
    #5 0x7fcbe4de6b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #6 0x560559a38439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV modules/swftext.c:225 swf_FontExtract_DefineFontInfo
==75376==ABORTING
```

## POC

SEGV-swf_FontExtract_DefineFontInfo-swftext-225.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