New issue

Jump to bottom

# A Segmentation fault in swfshape.c:783 #135

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
=================================================================
==10774==ERROR: AddressSanitizer: SEGV on unknown address 0x0000000000ba (pc 0x556daa02bdc9 bp 0x60400000df90 sp 0x7ffda9d04de0 T0)
    #0 0x556daa02bdc8 in swf_GetShapeBoundingBox modules/swfshape.c:783
    #1 0x556daa03b9d9 in swf_FontExtract_DefineFont2 modules/swftext.c:356
    #2 0x556daa03d414 in swf_FontExtract modules/swftext.c:602
    #3 0x556da9ffe5dc in fontcallback2 /home/seviezhou/swftools/src/swfdump.c:941
    #4 0x556daa036920 in swf_FontEnumerate modules/swftext.c:133
    #5 0x556da9ffb273 in main /home/seviezhou/swftools/src/swfdump.c:1296
    #6 0x7f03a464db96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x556da9ffe439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV modules/swfshape.c:783 swf_GetShapeBoundingBox
==10774==ABORTING
```

## POC

SEGV-swf_GetShapeBoundingBox-swfshape-783.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