New issue

Jump to bottom

A Segmentation fault in swftext.c:566 #142

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
=================================================================
==10761==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55e604db1be8 bp 0x000000000000 sp 0x7fff2eb65500 T0)
    #0 0x55e604db1be7 in updateusage modules/swftext.c:566
    #1 0x55e604da14f4 in swf_FontExtract_DefineTextCallback modules/swftext.c:516
    #2 0x55e604da9ffe in swf_FontUpdateUsage modules/swftext.c:578
    #3 0x55e604daa3c4 in swf_FontExtract modules/swftext.c:620
    #4 0x55e604d6b5dc in fontcallback2 /home/seviezhou/swftools/src/swfdump.c:941
    #5 0x55e604da3920 in swf_FontEnumerate modules/swftext.c:133
    #6 0x55e604d68273 in main /home/seviezhou/swftools/src/swfdump.c:1296
    #7 0x7f2499591b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #8 0x55e604d6b439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV modules/swftext.c:566 updateusage
==10761==ABORTING
```

POC

SEGV-updateusage-swftext-566.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