New issue

## A Segmentation fault in abc.c:772 #131



| Ubuntu x86,64, clang 6.0, swfdump (latest master fad6c2)  Command line  /src/swfdump - D @@  Output  ASAN: \$16560V  ***2802=#ER0R1: AddressSanitizer: \$560V on unknown address &e00000000000 (pc 0x7645887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 Te)  ### 2007-##### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-#### 2007-################################### | eviezhou commented on Aug 6, 2020   |
|--|---|
| Command line  /src/swfdump-D@@  Output  Segmentation fault (core dumped)  AddressSanitizer output  ASAN:SIGSEGV  | iystem info   |
| Output  Segmentation fault (core dumped)  AddressSanitizer output  ASAN:SIGSEGV  ***********************************   | buntu x86_64, clang 6.0, swfdump (latest master fad6c2)   |
| Segmentation fault (core dumped)  AddressSanitizer output  ASAN:SIGSEGV  | Command line  |
| AddressSanitizer output  ASAN:SIGSEGV  ==2802==ERROR: AddresSanitizer: SEGV on unknown address 0x0000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0)  #0 0x7f45887cf5s0 (/lib/x86_64-linux-gnu/lib.so.6+0x1865a0)  #1 0x7f4588cb1la8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8)  #2 0x55fe3061c083 in main / home/seviezhou/swftools/src/swfdump.c:1577  #4 0x7f4588662b06 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)  #5 0x55fe3062c0439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ??  ==2802==ABORTING   | src/swfdump -D @@   |
| ASAN:SIGSEGV  ===8802==ERROR: AddressSanitizer: SEGV on unknown address &xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   | Output  |
| ASAN:SIGSEGV ===2802==ERROR: AddresSsanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/1ib/x86_64-linux-gnu/libc.so.6+0x1865a0) #1 0x7f45887cf5a0 (xc)  | Segmentation fault (core dumped)  |
| ASAN:SIGSEGV ===2802==ERROR: AddresSsanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/1ib/x86_64-linux-gnu/libc.so.6+0x1865a0) #1 0x7f45887cf5a0 (xc)  |   |
| ==2802==ERROR: AddressSanitizer: SEGV on unknown address & 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/1ib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f45887cf5a1 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe30156341 in swf_ReadABC as3/abc.c:772 #3 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b06 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info. SUMMARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING   | AddressSanitizer output   |
| ==2802==ERROR: AddressSanitizer: SEGV on unknown address & 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/1ib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f45887cf5a1 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe30156341 in swf_ReadABC as3/abc.c:772 #3 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b06 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info. SUMMARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING   | tadi esssaintizer output  |
| ==2802==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/lib/x86_64-linux=gnu/libc.so.6+0x18e5a0) #1 0x7f45887cf5a0 in strdup (/usr/lib/x86_64-linux=gnu/libsan.so.2+0x621a8) #2 0x55fe300156341 in swf_ReadABC as3/abc.c:772 #3 0x55fe300156341 in swf_ReadABC as3/abc.c:772 #3 0x55fe300156003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b96 in _libc_start_main (/lib/x86_64-linux=gnu/libc.so.6+0x21b96) #5 0x55fe30016439 in _start (/home/seviezhou/swftools/src/swfdump+0x00439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING  | idal essessimilar da par  |
| #0 0x7f45887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f4588cb1la8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe30165411 in swf_Read&6 a3/abc.c:772 #3 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b06 inlibc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info. SLMWARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING  | ASAN: STGSEGV   |
| #2 0x55fe300156341 in swf_ReadABC as3/abc.c:772 #3 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x75fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING  | ASAN: SIGSEGV   |
| #3 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4580662b06 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0x00439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ?? #=2802==ABORTING  | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0)  |
| #4 0%7f4588662D96 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0%21D96) #5 0%55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0%d0439)  AddressSanitizer can not provide additional info.  SURMARY: AddressSanitizer: SEGV ??:0 ?? ==2802==ABORTING  | ASAN:SIGSEGV ===282==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7ff5887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f4588cb1la8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8)   |
| #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ??  ==2802==ABORTING   | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f4588cb11a8 in strdup (/usr/lib/x86_64-linux-gnu/libsan.so.2+0x621a8) #2 0x55fe30156341 in swf_ReadABC as3/abc.c:772  |
| SUMMARY: AddressSanitizer: SEGV ??:0 ??<br>==2802==ABORTING  | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address & xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx   |
| SUMMARY: AddressSanitizer: SEGV ??:0 ??<br>==2802==ABORTING  | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a1 in strdup (/usr/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f4588cb1a8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe30156341 in swf_ReadABC a33/abc.c:772 #3 0x55fe300cb033 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b96 in _libc_start_main //lib/x86_64-linux-gnu/libc.so.6+0x21b96)  |
| ==2802==ABORTING   | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address & x0e0e0e0e0e0e0e0 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195958 T0) #0 0x7f45887cf5a0 (/lib/x86.64-linux-gnu/libc.so.6+0x1865a0) #1 0x7f4588cb11a8 in strdup (/usr/lib/x86.4-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe3015641 in swf_ReadABC a33/abc.c:772 #3 0x55fe300cb003 in main / home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662b96 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  |
| POC  | ASAN:SIGSEGV ===2802==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff9195f958 T0) #0 0x7f45887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0) #1 0x7f4588cb1la8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8) #2 0x55fe30156341 in swf_ReadABC a3/abc.c:772 #3 0x55fe300cb030 in main /home/seviezhou/swftools/src/swfdump.c:1577 #4 0x7f4588662D96 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96) #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info. |
| POC  | ASAN:SIGSEGV  ==2802==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff91957958 T0)  #0 0x7f45887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0)  #1 0x7f4588Cb1a8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8)  #2 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577  #4 0x7f4588Cb96 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)  #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ??    |
|  | ASAN:SIGSEGV  ==2802==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000000 (pc 0x7f45887cf5a1 bp 0x7fff919601d0 sp 0x7fff91957958 T0)  #0 0x7f45887cf5a0 (/lib/x86_64-linux-gnu/libc.so.6+0x18e5a0)  #1 0x7f4588Cb1a8 in strdup (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x621a8)  #2 0x55fe300cb003 in main /home/seviezhou/swftools/src/swfdump.c:1577  #4 0x7f4588Cb96 in _libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)  #5 0x55fe300ce439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)  AddressSanitizer can not provide additional info.  SUMMARY: AddressSanitizer: SEGV ??:0 ??    |

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

⊙ Open

Assignees No one assigned Projects Milestone No milestone Development No branches or pull requests

1 participant

