New issue

Jump to bottom

A Segmentation fault in pool.c:1043 #136

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
=================================================================
==70016==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x55a36a93679a bp 0x60200000ec10 sp 0x7ffdfdb62ca0 T0)
    #0 0x55a36a936799 in pool_lookup_string2 as3/pool.c:1043
    #1 0x55a36a936d4a in constant_fromindex as3/pool.c:740
    #2 0x55a36a9299ad in swf_ReadABC as3/abc.c:789
    #3 0x55a36a89c003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #4 0x7fbc41038b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55a36a89f439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/pool.c:1043 pool_lookup_string2
==70016==ABORTING
```

POC

SEGV-pool_lookup_string2-pool-1043.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