New issue

Jump to bottom

A Segmentation fault in pool.c:300 #130

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
=================================================================
==4281==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x562d403c611d bp 0x60300000ebf8 sp 0x7ffd855128d0 T0)
    #0 0x562d403c611c in namespace_set_hash as3/pool.c:300
    #1 0x562d4045e879 in dict_put /home/seviezhou/swftools/lib/q.c:1146
    #2 0x562d4046486b in array_append /home/seviezhou/swftools/lib/q.c:1531
    #3 0x562d403d3337 in pool_read as3/pool.c:1160
    #4 0x562d403bef44 in swf_ReadABC as3/abc.c:748
    #5 0x562d40334003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #6 0x7fd1eca91b96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #7 0x562d40337439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/pool.c:300 namespace_set_hash
==4281==ABORTING
```

POC

SEGV-namespace_set_hash-pool-300.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