New issue

Jump to bottom

# A Segmentation fault in pool.c:1024 #138

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
=================================================================
==35659==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x55a669cff4d8 bp 0x60200000ed10 sp 0x7fffe1102550 T0)
    #0 0x55a669cff4d7 in pool_lookup_uint as3/pool.c:1024
    #1 0x55a669cffcda in constant_fromindex as3/pool.c:736
    #2 0x55a669cf2a1d in swf_ReadABC as3/abc.c:789
    #3 0x55a669c65003 in main /home/seviezhou/swftools/src/swfdump.c:1577
    #4 0x7ff7316aab96 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x21b96)
    #5 0x55a669c68439 in _start (/home/seviezhou/swftools/src/swfdump+0xd0439)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV as3/pool.c:1024 pool_lookup_uint
==35659==ABORTING
```

## POC

SEGV-pool_lookup_uint-pool-1024.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