SEGV in SWF::MethodBody::write(SWF::Writer*, SWF::Context*) #58

Open **Cvjark** opened this issue on Jul 11 · 0 comments

Cvjark commented on Jul 11

sample file

id11_SEGV_MethodBodywrite.zip

command to reproduce

```
./swfmill simple @@ /dev/null
```

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==56731==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x0000006b1554 bp
0x000000000001 sp 0x7fffd07b70c0 T0)
==56731==The signal is caused by a READ memory access.
==56731==Hint: address points to the zero page.
    #0 0x6b1554 in SWF::MethodBody::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/./SWFList.h
    #1 0x6b368d in SWF::Action3::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:2498:16
    #2 0x6cc70c in SWF::DoABCDefine::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:5377:10
    #3 0x6a2eac in SWF::Header::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:232:16
    #4 0x53d45c in SWF::File::save(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:158:11
    #5 0x54f8b9 in swfmill_xml2swf(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:251:21
    #6 0x7fa449fdac86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #7 0x4224d9 in _start (/home/bupt/Desktop/swfmill/src/swfmill+0x4224d9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swfmill/src/./SWFList.h in
```

```
SWF::MethodBody::write(SWF::Writer*, SWF::Context*)
==56731==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant