New issue

Jump to bottom

SEGV in SWF::DeclareFunction2::write(SWF::Writer*, SWF::Context*) #57

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

Cvjark commented on Jul 11

sample file

id41_SEGV_DeclareFunction2_write.zip

command to reproduce

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

crash detail

```
AddressSanitizer:DEADLYSIGNAL
=================================================================
==56747==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000008 (pc 0x0000006e2444 bp
0x0c16000002a0 sp 0x7ffd256ef030 T0)
==56747==The signal is caused by a READ memory access.
==56747==Hint: address points to the zero page.
    #0 0x6e2444 in SWF::DeclareFunction2::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/./SWFList.h
    #1 0x6c7dfc in SWF::DoInitAction::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:4858:16
    #2 0x6a2eac in SWF::Header::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:232:16
    #3 0x53d45c in SWF::File::save(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:158:11
    #4 0x54f8b9 in swfmill_xml2swf(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:251:21
    #5 0x7f99667cdc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #6 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::DeclareFunction2::write(SWF::Writer*, SWF::Context*)
==56747==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant