New issue

Jump to bottom

SEGV in SWF::Reader::getWord() #64

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

Cvjark commented on Jul 11

sample file

id4_SEGV_getWord.zip

command to reproduce

```
./swfmill swf2xml [sample file] /dev/null
```

crash detail

```
==55604==ERROR: AddressSanitizer: SEGV on unknown address 0x629feb002f56 (pc 0x0000005339a8 bp
0x000000bd0dc0 sp 0x7ffe0baa8310 T0)
==55604==The signal is caused by a READ memory access.
    #0 0x5339a8 in SWF::Reader::getWord() /home/bupt/Desktop/swfmill/src/SWFReader.cpp:46:11
    #1 0x540f06 in SWF::Tag::get(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFTag.cpp:8:24
    #2 0x61e75d in SWF::Header::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:432:13
    #3 0x53c76a in SWF::File::load(_IO_FILE*, SWF::Context*, unsigned int)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:88:11
    #4 0x54eda2 in swfmill_swf2xml(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:135:20
    #5 0x7f57e0760c86 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/SWFReader.cpp:46:11 in
SWF::Reader::getWord()
==55604==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant