heap-buffer-overflow in SWF::Reader::getU30() #61

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

Cvjark commented on Jul 11

sample file

id2_heap-buffer-overflow_getU30.zip

command to reproduce

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

crash detail

```
==55588==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62a0000051f3 at pc
0x000000534648 bp 0x7ffedf009d00 sp 0x7ffedf009cf8
READ of size 1 at 0x62a0000051f3 thread T0
    #0 0x534647 in SWF::Reader::getU30() /home/bupt/Desktop/swfmill/src/SWFReader.cpp:84:8
    #1 0x535d7a in SWF::Reader::getPStringU30()
/home/bupt/Desktop/swfmill/src/SWFReader.cpp:212:18
    #2 0x61c22a in SWF::String2::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:164:13
    #3 0x75d855 in SWF::String2::get(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFBasics.cpp:243:7
    #4 0x63d7d1 in SWF::Constants::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:3546:11
    #5 0x64010e in SWF::Action3::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:3676:12
    #6 0x672e50 in SWF::DoABC::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:8747:10
    #7 0x54120a in SWF::Tag::get(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFTag.cpp:29:8
    #8 0x61e75d in SWF::Header::parse(SWF::Reader*, int, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFParser.cpp:432:13
    #9 0x53c76a in SWF::File::load(_IO_FILE*, SWF::Context*, unsigned int)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:88:11
    #10 0x54eda2 in swfmill_swf2xml(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:135:20
    #11 0x7f3f0162dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
```

```
    #12 0x4224d9 in _start (/home/bupt/Desktop/swfmill/src/swfmill+0x4224d9)

0x62a0000051f3 is located 1 bytes to the right of 20466-byte region
[0x62a000000200,0x62a0000051f2)
allocated by thread T0 here:
    #0 0x4fa7c8 in operator new[](unsigned long) /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102
    #1 0x53c625 in SWF::File::load(_IO_FILE*, SWF::Context*, unsigned int)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:70:10
    #2 0x54eda2 in swfmill_swf2xml(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:135:20
    #3 0x7f3f0162dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swfmill/src/SWFReader.cpp:84:8
in SWF::Reader::getU30()
Shadow bytes around the buggy address:
  0x0c547fff89e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c547fff89f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c547fff8a00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c547fff8a10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c547fff8a20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c547fff8a30: 00 00 00 00 00 00 00 00 00 00 00 00 00[02]fa
  0x0c547fff8a40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fff8a50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fff8a60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fff8a70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c547fff8a80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==55588==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant