New issue

Jump to bottom

heap-buffer-overflow in SWF::Writer::writeByte(unsigned char) #56

Open **Cvjark** opened this issue on Jul 10 · 0 comments

Cvjark commented on Jul 10

sample file

id10_heap-buffer-overflow_writebyte.zip

command to reproduce

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

crash detail

```
=================================================================
==56715==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60b00000133e at pc
0x0000005376d4 bp 0x7ffc19fbb2d0 sp 0x7ffc19fbb2c8
WRITE of size 1 at 0x60b00000133e thread T0
    #0 0x5376d3 in SWF::Writer::writeByte(unsigned char)
/home/bupt/Desktop/swfmill/src/SWFWriter.cpp:269:15
    #1 0x5376d3 in SWF::Writer::putByte(unsigned char)
/home/bupt/Desktop/swfmill/src/SWFWriter.cpp:36:3
    #2 0x5418b1 in SWF::Action::writeHeader(SWF::Writer*, SWF::Context*, unsigned long)
/home/bupt/Desktop/swfmill/src/SWFAction.cpp:32:6
    #3 0x6d1324 in SWF::Play::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:5918:9
    #4 0x6ac96a in SWF::Event::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:1466:16
    #5 0x6c1d39 in SWF::PlaceObject2::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:4114:16
    #6 0x6a2eac in SWF::Header::write(SWF::Writer*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/gSWFWriter.cpp:232:16
    #7 0x53d45c in SWF::File::save(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:158:11
    #8 0x54f8b9 in swfmill_xml2swf(int, char**) /home/bupt/Desktop/swfmill/src/swfmill.cpp:251:21
    #9 0x7f631bcfdc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
```

```
    #10 0x4224d9 in _start (/home/bupt/Desktop/swfmill/src/swfmill+0x4224d9)

0x60b00000133e is located 0 bytes to the right of 110-byte region [0x60b0000012d0,0x60b00000133e)
allocated by thread T0 here:
    #0 0x4fa7c8 in operator new[](unsigned long) /home/bupt/桌面/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_new_delete.cpp:102
    #1 0x53d3ae in SWF::File::save(_IO_FILE*, SWF::Context*)
/home/bupt/Desktop/swfmill/src/SWFFile.cpp:149:10

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swfmill/src/SWFWriter.cpp:269:15 in SWF::Writer::writeByte(unsigned char)
Shadow bytes around the buggy address:
  0x0c167fff8210: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c167fff8220: 00 00 00 00 06 fa fa fa fa fa fa fa fa fa 00 00
  0x0c167fff8230: 00 00 00 00 00 00 00 00 00 00 07 fa fa fa fa
  0x0c167fff8240: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c167fff8250: 00 07 fa fa fa fa fa fa fa fa 00 00 00 00 00 00
=>0x0c167fff8260: 00 00 00 00 00 00 00[06]fa fa fa fa fa fa fa
  0x0c167fff8270: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8280: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff8290: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff82a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c167fff82b0: 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
==56715==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant