New issue

Jump to bottom

bug found in swfrender #185

Open **Cvjark** opened this issue on Jul 4 · 0 comments

Cvjark commented on Jul 4

swfrender

heap buffer overflow

command to reproduce

```
./swfrender [sample file] -o /dev/null
```

crash sample

id8_heap-buffer-overflow_swf_DefineLosslessBitsTagToImage.zip

crash info

```
==20010==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6110000007fc at pc
0x000000509052 bp 0x7ffd07ab6370 sp 0x7ffd07ab6368
READ of size 4 at 0x6110000007fc thread T0
    #0 0x509051 in swf_DefineLosslessBitsTagToImage
/home/bupt/Desktop/swftools/lib/modules/swfbits.c:1037:16
    #1 0x50aacb in swf_ExtractImage /home/bupt/Desktop/swftools/lib/modules/swfbits.c:1221:9
    #2 0x4fcf44 in extractDefinitions /home/bupt/Desktop/swftools/lib/readers/swf.c:405:18
    #3 0x4fcf44 in swf_open /home/bupt/Desktop/swftools/lib/readers/swf.c:736:18
    #4 0x4f6846 in main /home/bupt/Desktop/swftools/src/swfrender.c:174:29
    #5 0x7fb150d57c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #6 0x41d4c9 in _start (/home/bupt/Desktop/swftools/build/bin/swfrender+0x41d4c9)

0x6110000007fc is located 764 bytes to the right of 256-byte region
[0x611000000400,0x611000000500)
allocated by thread T0 here:
    #0 0x4afa90 in malloc /home/bupt/桌面/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
```

```
    #1 0x62146e in rfx_alloc /home/bupt/Desktop/swftools/lib/mem.c:30:9
    #2 0x50aacb in swf_ExtractImage /home/bupt/Desktop/swftools/lib/modules/swfbits.c:1221:9
    #3 0x4f6846 in main /home/bupt/Desktop/swftools/src/swfrender.c:174:29
    #4 0x7fb150d57c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/lib/modules/swfbits.c:1037:16 in swf_DefineLosslessBitsTagToImage
Shadow bytes around the buggy address:
  0x0c227fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff80e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c227fff80f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa[fa]
  0x0c227fff8100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8110: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c227fff8140: 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
==20010==ABORTING
```

SEGV

command to reproduce

```
./swfrender [sample file] -o /dev/null
```

crash sample

id58_SEGV_extractFrame.zip

crash info

```
==20817==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000004 (pc 0x0000004f9f76 bp
0x0c1600000664 sp 0x7fffe97402a0 T0)
==20817==The signal is caused by a READ memory access.
==20817==Hint: address points to the zero page.
    #0 0x4f9f76 in extractFrame /home/bupt/Desktop/swftools/lib/readers/swf.c:458:49
    #1 0x4f981c in swfpage_render /home/bupt/Desktop/swftools/lib/readers/swf.c:637:23
    #2 0x4f7398 in main /home/bupt/Desktop/swftools/src/swfrender.c:218:17
    #3 0x7f720636dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #4 0x41d4c9 in _start (/home/bupt/Desktop/swftools/build/bin/swfrender+0x41d4c9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/readers/swf.c:458:49 in
extractFrame
==20817==ABORTING
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant