Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034381/id0_heap-buffer-overflow.zip

Command to reproduce

```
./png2swf -j 50 [sample file] -o /dev/null
```

Product name & version

```
last github commit code : 772e55a
```

Problem Type

```
heap-buffer-overflow
```

Crash Detail

```
==109951==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000001c
at pc 0x0000004f680f bp 0x7ffde7515f90 sp 0x7ffde7515f88
READ of size 1 at 0x60200000001c thread T0
    #0 0x4f680e in png_read_header
/home/bupt/Desktop/swftools/src/png2swf.c:184:10
    #1 0x4fbbf8 in CheckInputFile /home/bupt/Desktop/swftools/src/png2swf.c:583:9
    #2 0x4fca4e in args_callback_command
/home/bupt/Desktop/swftools/src/png2swf.c:754:9
    #3 0x4fcfd4 in processargs
/home/bupt/Desktop/swftools/src/./../lib/args.h:89:16
    #4 0x4fcfd4 in main /home/bupt/Desktop/swftools/src/png2swf.c:802:5
    #5 0x7fc97197cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #6 0x41ce29 in _start
(/home/bupt/Desktop/swftools/build/bin/png2swf+0x41ce29)

0x60200000001c is located 0 bytes to the right of 12-byte region
[0x602000000010,0x60200000001c)
allocated by thread T0 here:
    #0 0x4af3f0 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f579b in png_read_chunk
/home/bupt/Desktop/swftools/src/png2swf.c:127:18
    #2 0x4f5cc6 in png_read_header
/home/bupt/Desktop/swftools/src/png2swf.c:170:11
    #3 0x4fbbf8 in CheckInputFile /home/bupt/Desktop/swftools/src/png2swf.c:583:9
    #4 0x4fca4e in args_callback_command
/home/bupt/Desktop/swftools/src/png2swf.c:754:9
    #5 0x4fcfd4 in processargs
/home/bupt/Desktop/swftools/src/./../lib/args.h:89:16
    #6 0x4fcfd4 in main /home/bupt/Desktop/swftools/src/png2swf.c:802:5
    #7 0x7fc97197cc86 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/src/png2swf.c:184:10 in png_read_header
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa 00[04]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: 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
==109951==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/src/png2swf.c:184:10 in png_read_header
```