Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ···

main ···

Poc / swftools / gif2swf / CVE-2022-35089.md

Cvjark Create CVE-2022-35089.md History

1 contributor

75 lines (66 sloc) | 2.96 KB ···

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034336/id47_HEAP_BUFFER_OVERFLOW.zip

Command to reproduce

```
./gif2swf -o /dev/null [sample file]
```

Product name & version

`last github commit code : 772e55a`

Problem Type

```
heap-buffer-overflow
```

Crash Detail

```
==117675==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000065f3
at pc 0x0000004f95d9 bp 0x7ffe740a8c50 sp 0x7ffe740a8c48
READ of size 1 at 0x6020000065f3 thread T0
    #0 0x4f95d8 in getTransparentColor
/home/bupt/Desktop/swftools/src/gif2swf.c:141:20
    #1 0x4f95d8 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:269:20
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7f7d9a8e5c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #4 0x41cfb9 in _start
(/home/bupt/Desktop/swftools/build/bin/gif2swf+0x41cfb9)

0x6020000065f3 is located 0 bytes to the right of 3-byte region
[0x6020000065f0,0x6020000065f3)
allocated by thread T0 here:
    #0 0x4af580 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x7f7d9c21919a in GifAddExtensionBlock (/usr/lib/x86_64-linux-
gnu/libgif.so.7+0x519a)

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/src/gif2swf.c:141:20 in getTransparentColor
Shadow bytes around the buggy address:
  0x0c047fff8c60: fa fa 06 fa fa fa 04 fa fa fa fd fd fa fa 00 04
  0x0c047fff8c70: fa fa 00 00 fa fa 06 fa fa fa 04 fa fa fa 00 00
  0x0c047fff8c80: fa fa 06 fa fa fa 04 fa fa fa 04 fa fa fa 00 00
  0x0c047fff8c90: fa fa 06 fa fa fa 04 fa fa fa 04 fa fa fa 00 03
  0x0c047fff8ca0: fa fa 03 fa fa fa 04 fa fa fa 00 00 fa fa 01 fa
=>0x0c047fff8cb0: fa fa 06 fa fa fa 04 fa fa fa 03 fa fa fa[03]fa
  0x0c047fff8cc0: fa fa 01 fa fa fa 06 fa fa fa 04 fa fa fa 04 fa
  0x0c047fff8cd0: fa fa 00 00 fa fa 06 fa fa fa 04 fa fa fa fa fa
  0x0c047fff8ce0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8cf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8d00: 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
==117675==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/src/gif2swf.c:141:20 in getTransparentColor
```