Cvjark / Poc Public

Code Issues 1 Pull requests Actions Projects Security ...

main

Poc / swftools / gif2swf / CVE-2022-35088.md

Cvjark Create CVE-2022-35088.md History

1 contributor

75 lines (66 sloc) | 2.94 KB

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034335/id39_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

```
==117565==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000271
at pc 0x0000004f9626 bp 0x7ffd465ed6d0 sp 0x7ffd465ed6c8
READ of size 1 at 0x602000000271 thread T0
    #0 0x4f9625 in getGifDelayTime
/home/bupt/Desktop/swftools/src/gif2swf.c:127:20
    #1 0x4f9625 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:451:17
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7ff0fa7dbc86 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)

0x602000000271 is located 0 bytes to the right of 1-byte region
[0x602000000270,0x602000000271)
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 0x7ff0fc10f19a in GifAddExtensionBlock (/usr/lib/x86_64-linux-
gnu/libgif.so.7+0x519a)

SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/src/gif2swf.c:127:20 in getGifDelayTime
Shadow bytes around the buggy address:
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c047fff8010: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fd
  0x0c047fff8020: fa fa fd fd fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8030: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 00 04
=>0x0c047fff8040: fa fa 00 03 fa fa 03 fa fa fa 04 fa fa fa[01]fa
  0x0c047fff8050: fa fa 06 fa fa fa 04 fa fa fa 01 fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8090: 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
==117565==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow
/home/bupt/Desktop/swftools/src/gif2swf.c:127:20 in getGifDelayTime
```