Cvjark Create CVE-2022-35090.md History

1 contributor

77 lines (68 sloc) | 3.28 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034327/id1_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

```
==32466==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000964
at pc 0x0000004ae3e4 bp 0x7ffce30cd590 sp 0x7ffce30ccd40
WRITE of size 8 at 0x619000000964 thread T0
    #0 0x4ae3e3 in __asan_memcpy /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
    #1 0x4f8002 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:328:25
    #2 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #3 0x7f9f1d7dec86 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)

0x619000000964 is located 4 bytes to the right of 992-byte region
[0x619000000580,0x619000000960)
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 0x4f698e in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:310:29
    #2 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #3 0x7f9f1d7dec86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
in __asan_memcpy
Shadow bytes around the buggy address:
  0x0c327fff80d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff80e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8120: 00 00 00 00 00 00 00 00 00 00 00 00[fa]fa fa fa
  0x0c327fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8160: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff8170: 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
==32466==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
in __asan_memcpy
```