Cvjark Create CVE-2022-35086.md History

1 contributor

42 lines (33 sloc) | 1.49 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034338/id31_SEGV.zip

Command to reproduce

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

Product name & version

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

Problem Type

```
SEGV
```

Crash Detail

```
AddressSanitizer:DEADLYSIGNAL
==117415==ERROR: AddressSanitizer: SEGV on unknown address 0x61e000016efe (pc
0x7fb8e4a4e246 bp 0x7ffc023949b0 sp 0x7ffc02394148 T0)
==117415==The signal is caused by a WRITE memory access.
    #0 0x7fb8e4a4e246  /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:309
    #1 0x4ae15b in __asan_memcpy /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cpp:22
    #2 0x4f8251 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:353:25
    #3 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #4 0x7fb8e49b4c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #5 0x41cfb9 in _start
(/home/bupt/Desktop/swftools/build/bin/gif2swf+0x41cfb9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:309
==117415==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV /build/glibc-CVJwZb/glibc-
2.27/string/../sysdeps/x86_64/multiarch/memmove-vec-unaligned-erms.S:309
```