Cvjark Create CVE-2022-35087.md History

1 contributor

40 lines (32 sloc) | 1.2 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034337/id0_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
==32434==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc
0x0000004f63a0 bp 0x7ffe31857cb0 sp 0x7ffe31857ae0 T0)
==32434==The signal is caused by a READ memory access.
==32434==Hint: address points to the zero page.
    #0 0x4f63a0 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:268:27
    #1 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #2 0x7fd91af28c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #3 0x41cfb9 in _start
(/home/bupt/Desktop/swftools/build/bin/gif2swf+0x41cfb9)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/src/gif2swf.c:268:27
in MovieAddFrame
==32434==ABORTING
```

Crash summary

```
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/src/gif2swf.c:268:27
in MovieAddFrame
```