Cvjark Create CVE-2022-35080.md History

1 contributor

38 lines (28 sloc) | 1.11 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034385/id12_SEGV.zip

Command to reproduce

```
./png2swf -j 50 [sample file] -o /dev/null
```

Product name & version

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

Problem Type

```
SEGV
```

Crash Detail

```
AddressSanitizer:DEADLYSIGNAL

==30779==ERROR: AddressSanitizer: SEGV on unknown address 0x7f62129fc800 (pc
0x000000550c36 bp 0x7ffc5ce7ea10 sp 0x7ffc5ce7e780 T0)
==30779==The signal is caused by a READ memory access.
    #0 0x550c36 in png_load /home/bupt/Desktop/swftools/lib/png.c:801:17
    #1 0x4fac8f in MovieAddFrame /home/bupt/Desktop/swftools/src/png2swf.c:476:6
    #2 0x4fd5f5 in main /home/bupt/Desktop/swftools/src/png2swf.c:822:10
    #3 0x7f6316332c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310
    #4 0x41ce29 in _start
(/home/bupt/Desktop/swftools/build/bin/png2swf+0x41ce29)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/bupt/Desktop/swftools/lib/png.c:801:17 in
png_load
==30779==ABORTING
```