Cvjark Create CVE-2022-35085.md History

1 contributor

87 lines (69 sloc) | 4.48 KB ...

Product Link

https://github.com/matthiaskramm/swftools

POC file

https://github.com/matthiaskramm/swftools/files/9034341/id15_memory_leak.zip

Command to reproduce

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

Product name & version

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

Problem Type

```
memory leaks
```

Crash Detail

```
==32723==ERROR: LeakSanitizer: detected memory leaks

Direct leak of 56 byte(s) in 1 object(s) allocated from:
    #0 0x4af748 in calloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:154
    #1 0x588b93 in rfx_calloc /home/bupt/Desktop/swftools/lib/mem.c:69:9
    #2 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #3 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Direct leak of 56 byte(s) in 1 object(s) allocated from:
    #0 0x4af748 in calloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:154
    #1 0x588b93 in rfx_calloc /home/bupt/Desktop/swftools/lib/mem.c:69:9
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x4af580 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x58897e in rfx_alloc /home/bupt/Desktop/swftools/lib/mem.c:30:9
    #2 0x51e69a in swf_ShapeAddBitmapFillStyle
/home/bupt/Desktop/swftools/lib/modules/swfshape.c:312:10
    #3 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #4 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x4af580 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x58897e in rfx_alloc /home/bupt/Desktop/swftools/lib/mem.c:30:9
    #2 0x51e69a in swf_ShapeAddBitmapFillStyle
/home/bupt/Desktop/swftools/lib/modules/swfshape.c:312:10
    #3 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #4 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: 240 byte(s) leaked in 4 allocation(s).
info: No menu item '=' in node '(dir)Top'==32723==ERROR: LeakSanitizer: detected
memory leaks

Direct leak of 56 byte(s) in 1 object(s) allocated from:
    #0 0x4af748 in calloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:154
    #1 0x588b93 in rfx_calloc /home/bupt/Desktop/swftools/lib/mem.c:69:9
```

```
    #2 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #3 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Direct leak of 56 byte(s) in 1 object(s) allocated from:
    #0 0x4af748 in calloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:154
    #1 0x588b93 in rfx_calloc /home/bupt/Desktop/swftools/lib/mem.c:69:9
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x4af580 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x58897e in rfx_alloc /home/bupt/Desktop/swftools/lib/mem.c:30:9
    #2 0x51e69a in swf_ShapeAddBitmapFillStyle
/home/bupt/Desktop/swftools/lib/modules/swfshape.c:312:10
    #3 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #4 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

Indirect leak of 64 byte(s) in 1 object(s) allocated from:
    #0 0x4af580 in malloc /home/bupt/Desktop/tools/llvm-
12.0.1/llvm/projects/compiler-rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x58897e in rfx_alloc /home/bupt/Desktop/swftools/lib/mem.c:30:9
    #2 0x51e69a in swf_ShapeAddBitmapFillStyle
/home/bupt/Desktop/swftools/lib/modules/swfshape.c:312:10
    #3 0x4fb951 in main /home/bupt/Desktop/swftools/src/gif2swf.c:728:17
    #4 0x7fb865a10c86 in __libc_start_main /build/glibc-CVJwZb/glibc-
2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: 240 byte(s) leaked in 4 allocation(s).
```

Crash summary

```
SUMMARY: AddressSanitizer: 240 byte(s) leaked in 4 allocation(s).
```