New issue

Jump to bottom

bug found in swftools-gif2swf #181

Open **Cvjark** opened this issue on Jul 3 · 0 comments

Cvjark commented on Jul 3 • edited

Hi, I currently learn to use fuzz tech to detect bugs and I found something in this repo.
in order to reproduce the crash info, please attach ASAN when you compile this repo.

gif2swf

heap-buffer-overflow

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id1_HEAP_BUFFER_OVERFLOW.zip

crash info

```
==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
```

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id39_HEAP_BUFFER_OVERFLOW.zip

crash info

```
==117565==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x602000000271 at pc
0x0000004f9626 bp 0x7ffd465ed6d0 sp 0x7ffd465ed6c8
READ of size 1 at 0x602000000271 thread T0
    #0 0x4f9625 in getGifDelayTime /home/bupt/Desktop/swftools/src/gif2swf.c:127:20
    #1 0x4f9625 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:451:17
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7ff0fa7dbc86 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)

0x602000000271 is located 0 bytes to the right of 1-byte region [0x602000000270,0x602000000271)
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 0x7ff0fc10f19a in GifAddExtensionBlock (/usr/lib/x86_64-linux-gnu/libgif.so.7+0x519a)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/src/gif2swf.c:127:20
in getGifDelayTime
Shadow bytes around the buggy address:
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff8000: fa fa fd fd fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c047fff8010: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fd
  0x0c047fff8020: fa fa fd fd fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8030: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 00 04
=>0x0c047fff8040: fa fa 00 03 fa fa 03 fa fa fa 04 fa fa fa[01]fa
  0x0c047fff8050: fa fa 06 fa fa fa 04 fa fa fa 01 fa fa fa fa fa
  0x0c047fff8060: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8090: 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
==117565==ABORTING
```

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id47_HEAP_BUFFER_OVERFLOW.zip

crash info

```
==117675==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000065f3 at pc
0x0000004f95d9 bp 0x7ffe740a8c50 sp 0x7ffe740a8c48
READ of size 1 at 0x6020000065f3 thread T0
    #0 0x4f95d8 in getTransparentColor /home/bupt/Desktop/swftools/src/gif2swf.c:141:20
    #1 0x4f95d8 in MovieAddFrame /home/bupt/Desktop/swftools/src/gif2swf.c:269:20
    #2 0x4fb9d9 in main /home/bupt/Desktop/swftools/src/gif2swf.c:730:21
    #3 0x7f7d9a8e5c86 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)

0x6020000065f3 is located 0 bytes to the right of 3-byte region [0x6020000065f0,0x6020000065f3)
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 0x7f7d9c21919a in GifAddExtensionBlock (/usr/lib/x86_64-linux-gnu/libgif.so.7+0x519a)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/src/gif2swf.c:141:20
in getTransparentColor
Shadow bytes around the buggy address:
  0x0c047fff8c60: fa fa 06 fa fa fa 04 fa fa fa fd fd fa fa 00 04
  0x0c047fff8c70: fa fa 00 00 fa fa 06 fa fa fa 04 fa fa fa 00 00
  0x0c047fff8c80: fa fa 06 fa fa fa 04 fa fa fa 04 fa fa fa 00 00
  0x0c047fff8c90: fa fa 06 fa fa fa 04 fa fa fa 04 fa fa fa 00 03
  0x0c047fff8ca0: fa fa 03 fa fa fa 04 fa fa fa 00 00 fa fa 01 fa
=>0x0c047fff8cb0: fa fa 06 fa fa fa 04 fa fa fa 03 fa fa fa[03]fa
  0x0c047fff8cc0: fa fa 01 fa fa fa 06 fa fa fa 04 fa fa fa 04 fa
  0x0c047fff8cd0: fa fa 00 00 fa fa 06 fa fa fa 04 fa fa fa fa fa
  0x0c047fff8ce0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8cf0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8d00: 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
==117675==ABORTING
```

SEGV

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id0_SEGV.zip

crash info

```
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
```

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id31_SEGV.zip

crash info

```
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
```

memory leak

reproduce

please use command : `./gif2swf -o /dev/null [sample file]` to reproduce the crash

crash_sample

id15_memory_leak.zip

crash info

```
==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).
```

Cvjark changed the title ~~**bug found in swftools**~~ **bug found in swftools-gif2swf** on Jul 3

Cvjark mentioned this issue on Jul 3

bug report swftools-pdf2swf #184

Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant