New issue

Jump to bottom

bug found in swftools-png2swf #183

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.

heap buffer overflow

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id0_heap-buffer-overflow.zip

crash info

```
==109951==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200000001c at pc
0x0000004f680f bp 0x7ffde7515f90 sp 0x7ffde7515f88
READ of size 1 at 0x60200000001c thread T0
    #0 0x4f680e in png_read_header /home/bupt/Desktop/swftools/src/png2swf.c:184:10
    #1 0x4fbbf8 in CheckInputFile /home/bupt/Desktop/swftools/src/png2swf.c:583:9
    #2 0x4fca4e in args_callback_command /home/bupt/Desktop/swftools/src/png2swf.c:754:9
    #3 0x4fcfd4 in processargs /home/bupt/Desktop/swftools/src/./../lib/args.h:89:16
    #4 0x4fcfd4 in main /home/bupt/Desktop/swftools/src/png2swf.c:802:5
    #5 0x7fc97197cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310
    #6 0x41ce29 in _start (/home/bupt/Desktop/swftools/build/bin/png2swf+0x41ce29)

0x60200000001c is located 0 bytes to the right of 12-byte region [0x602000000010,0x60200000001c)
allocated by thread T0 here:
    #0 0x4af3f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x4f579b in png_read_chunk /home/bupt/Desktop/swftools/src/png2swf.c:127:18
    #2 0x4f5cc6 in png_read_header /home/bupt/Desktop/swftools/src/png2swf.c:170:11
```

```
    #3 0x4fbbf8 in CheckInputFile /home/bupt/Desktop/swftools/src/png2swf.c:583:9
    #4 0x4fca4e in args_callback_command /home/bupt/Desktop/swftools/src/png2swf.c:754:9
    #5 0x4fcfd4 in processargs /home/bupt/Desktop/swftools/src/./../lib/args.h:89:16
    #6 0x4fcfd4 in main /home/bupt/Desktop/swftools/src/png2swf.c:802:5
    #7 0x7fc97197cc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/src/png2swf.c:184:10
in png_read_header
Shadow bytes around the buggy address:
  0x0c047fff7fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c047fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c047fff8000: fa fa 00[04]fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: 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
==109951==ABORTING
```

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id5_heap-buffer-overflow.zip

crash info

```
==7560==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6190000004a1 at pc
0x000000552b5b bp 0x7ffc4a0c7730 sp 0x7ffc4a0c7728
READ of size 1 at 0x6190000004a1 thread T0
    #0 0x552b5a in png_load /home/bupt/Desktop/swftools/lib/png.c:813:15
    #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 0x7fbc1782dc86 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)

0x6190000004a1 is located 0 bytes to the right of 1057-byte region [0x619000000080,0x6190000004a1)
allocated by thread T0 here:
    #0 0x4af3f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x54bf0e in png_load /home/bupt/Desktop/swftools/lib/png.c:517:33
    #2 0x4fac8f in MovieAddFrame /home/bupt/Desktop/swftools/src/png2swf.c:476:6
    #3 0x4fd5f5 in main /home/bupt/Desktop/swftools/src/png2swf.c:822:10
    #4 0x7fbc1782dc86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/lib/png.c:813:15 in
png_load
Shadow bytes around the buggy address:
  0x0c327fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8070: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff8090: 00 00 00 00[01]fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff80e0: 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
==7560==ABORTING
```

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id8_heap_buffer_overflow.zip

crash info

```
==16841==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000001b4 at pc
0x000000552ceb bp 0x7fff18453570 sp 0x7fff18453568
READ of size 4 at 0x6020000001b4 thread T0
    #0 0x552cea in png_load /home/bupt/Desktop/swftools/lib/png.c:832:43
    #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 0x7f90177d9c86 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)

0x6020000001b4 is located 0 bytes to the right of 4-byte region [0x6020000001b0,0x6020000001b4)
allocated by thread T0 here:
    #0 0x4af3f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x55014c in png_load /home/bupt/Desktop/swftools/lib/png.c:768:19
    #2 0x4fac8f in MovieAddFrame /home/bupt/Desktop/swftools/src/png2swf.c:476:6
    #3 0x4fd5f5 in main /home/bupt/Desktop/swftools/src/png2swf.c:822:10
    #4 0x7f90177d9c86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/lib/png.c:832:43 in
png_load
Shadow bytes around the buggy address:
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  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 fa fa fa fd fd fa fa 00 05
  0x0c047fff8010: fa fa fd fd fa fa fd fa fa fa fd fd fa fa 00 05
  0x0c047fff8020: fa fa fd fd fa fa 03 fa fa fa fd fd fa fa fd fd
=>0x0c047fff8030: fa fa 00 05 fa fa[04]fa fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa 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
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
==16841==ABORTING
```

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id13_heap-buffer-overflow.zip

crash info

```
==39505==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x617000000378 at pc
0x000000552c2e bp 0x7fff87bf0950 sp 0x7fff87bf0948
READ of size 4 at 0x617000000378 thread T0
    #0 0x552c2d in png_load /home/bupt/Desktop/swftools/lib/png.c:832:43
    #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 0x7f3352dcec86 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)

0x617000000378 is located 68 bytes to the right of 692-byte region [0x617000000080,0x617000000334)
allocated by thread T0 here:
    #0 0x4af3f0 in malloc /home/bupt/Desktop/tools/llvm-12.0.1/llvm/projects/compiler-
rt/lib/asan/asan_malloc_linux.cpp:145
    #1 0x55014c in png_load /home/bupt/Desktop/swftools/lib/png.c:768:19
    #2 0x4fac8f in MovieAddFrame /home/bupt/Desktop/swftools/src/png2swf.c:476:6
    #3 0x4fd5f5 in main /home/bupt/Desktop/swftools/src/png2swf.c:822:10
    #4 0x7f3352dcec86 in __libc_start_main /build/glibc-CVJwZb/glibc-2.27/csu/../csu/libc-
start.c:310

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/bupt/Desktop/swftools/lib/png.c:832:43 in
png_load
Shadow bytes around the buggy address:
```

```
  0x0c2e7fff8010: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2e7fff8050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2e7fff8060: 00 00 00 00 00 00 04 fa fa fa fa fa fa fa fa[fa]
  0x0c2e7fff8070: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8080: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff8090: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff80a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2e7fff80b0: 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
==39505==ABORTING
```

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id16_heap-buffer-overflow.zip

crash info

```
==29029==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000001b8 at pc
0x000000552ceb bp 0x7ffc959816f0 sp 0x7ffc959816e8
READ of size 4 at 0x6020000001b8 thread T0
==29029==WARNING: failed to fork (errno 12)
==29029==WARNING: failed to fork (errno 12)
==29029==WARNING: failed to fork (errno 12)
==29029==WARNING: failed to fork (errno 12)
==29029==WARNING: failed to fork (errno 12)
```

```
==29029==WARNING: Failed to use and restart external symbolizer!
    #0 0x552cea  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x552cea)
    #1 0x4fac8f  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x4fac8f)
    #2 0x4fd5f5  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x4fd5f5)
    #3 0x7f324745ac86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)
    #4 0x41ce29  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x41ce29)

0x6020000001b8 is located 4 bytes to the right of 4-byte region [0x6020000001b0,0x6020000001b4)
allocated by thread T0 here:
    #0 0x4af3f0  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x4af3f0)
    #1 0x55014c  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x55014c)
    #2 0x4fac8f  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x4fac8f)
    #3 0x4fd5f5  (/home/bupt/Desktop/swftools/build/bin/png2swf+0x4fd5f5)
    #4 0x7f324745ac86  (/lib/x86_64-linux-gnu/libc.so.6+0x21c86)

SUMMARY: AddressSanitizer: heap-buffer-overflow
(/home/bupt/Desktop/swftools/build/bin/png2swf+0x552cea)
Shadow bytes around the buggy address:
  0x0c047fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  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 fa fa fa fd fd fa fa fd fd
  0x0c047fff8010: fa fa fd fd fa fa fd fa fa fa fd fd fa fa fd fd
  0x0c047fff8020: fa fa fd fd fa fa 03 fa fa fa fd fd fa fa fd fd
=>0x0c047fff8030: fa fa fd fd fa fa 04[fa]fa fa fa fa fa fa fa fa
  0x0c047fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8050: fa fa fa fa fa fa fa fa fa fa fa 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
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
```

SEGV

reproduce

command to reproduce the crash : ./png2swf -j 50 [sample file] -o /dev/null

sample file

id12_SEGV.zip

crash info

```
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
```


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