New issue

Jump to bottom

heap overflow in decompileIF decompile.c:2436 #197

Open **cuanduo** opened this issue on Apr 16, 2020 · 0 comments

cuanduo commented on Apr 16, 2020

./swftocxx $poc

segmentaion_fault_decompile_569-out_of_bound-idx:0x1186-0x10.zip

```
root@ubuntu:/home/tim/libming/util# ../../libming-asan/util/swftocxx overflows/segmentaion_fault_decompile_569-out_of_bound-idx\:0x1186-0x10
header indicates a filesize of 1484 but filesize is 228
#include <mingpp.h>


main(){
SWFMovie* m = new SWFMovie(10);

Ming_setScale(1.0);
m->setRate(24.000000);
m->setDimension(-9480, 8000);

// SWF_PLACEOBJECT3
 Stream out of sync after parse of blocktype 12 (SWF_DOACTION). 223 but expecting 200.

// SWF_DOACTION
=================================================================
==3292==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61f000000c70 at pc 0x561ec3153e3b bp 0x7fff7af46a10 sp 0x7fff7af46a00
READ of size 2 at 0x61f000000c70 thread T0
    #0 0x561ec3153e3a in decompileIF /home/tim/libming-asan/util/decompile.c:2436
    #1 0x561ec3158ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
    #2 0x561ec315932e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
    #3 0x561ec3152d13 in decompile_SWITCH /home/tim/libming-asan/util/decompile.c:2235
    #4 0x561ec3154f7b in decompileIF /home/tim/libming-asan/util/decompile.c:2594
    #5 0x561ec3158ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
    #6 0x561ec315932e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
    #7 0x561ec3159464 in decompile5Action /home/tim/libming-asan/util/decompile.c:3517
    #8 0x561ec314548e in outputSWF_DOACTION /home/tim/libming-asan/util/outputscript.c:1551
    #9 0x561ec3147a92 in outputBlock /home/tim/libming-asan/util/outputscript.c:2083
    #10 0x561ec3148b88 in readMovie /home/tim/libming-asan/util/main.c:281
    #11 0x561ec3149322 in main /home/tim/libming-asan/util/main.c:354
    #12 0x7faeb56eab6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
    #13 0x561ec313b469 in _start (/home/tim/libming-asan/util/.libs/swftocxx+0x14469)

0x61f000000c70 is located 16 bytes to the right of 3040-byte region [0x61f000000080,0x61f000000c60)
allocated by thread T0 here:
    #0 0x7faeb5c3d63e in calloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10c63e)
    #1 0x561ec3154e26 in decompileIF /home/tim/libming-asan/util/decompile.c:2587
    #2 0x561ec3158ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
    #3 0x561ec315932e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
    #4 0x561ec3159464 in decompile5Action /home/tim/libming-asan/util/decompile.c:3517
    #5 0x561ec314548e in outputSWF_DOACTION /home/tim/libming-asan/util/outputscript.c:1551
    #6 0x561ec3147a92 in outputBlock /home/tim/libming-asan/util/outputscript.c:2083
    #7 0x561ec3148b88 in readMovie /home/tim/libming-asan/util/main.c:281
    #8 0x561ec3149322 in main /home/tim/libming-asan/util/main.c:354
    #9 0x7faeb56eab6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/tim/libming-asan/util/decompile.c:2436 in decompileIF
Shadow bytes around the buggy address:
  0x0c3e7fff8130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3e7fff8140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3e7fff8150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3e7fff8160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c3e7fff8170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c3e7fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 fa fa[fa]fa
  0x0c3e7fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3e7fff81a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3e7fff81b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3e7fff81c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3e7fff81d0: 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
==3292==ABORTING
root@ubuntu:/home/tim/libming/util#
```

cxlzff mentioned this issue on Jun 26, 2021

stack-overflow in parseSWF_ACTIONRECORD(util/parser.c:1166) #229

⊙ Open

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant