

New issue

[Jump to bottom](#)

heap overflow in decompileIF decompile.c:2473 #196



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-idx0x1199-0xb.zip](#)

```
root@ubuntu:/home/tim/libming/util# ../libming-asan/util/swftocxx overflows/segmentaion_fault_decompile_569-out_of_bound-idx\0x1199-0xb
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
    =====
==3097==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61d0000008a8 at pc 0x5645c2842407 bp 0x7fffd6e8470 sp 0x7fffd6e8460
READ of size 8 at 0x61d0000008a8 thread T0
#0 0x5645c2842406 in decompileIF /home/tim/libming-asan/util/decompile.c:2473
#1 0x5645c2846ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
#2 0x5645c284732e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
#3 0x5645c28467ee in decompileSETTARGET /home/tim/libming-asan/util/decompile.c:3169
#4 0x5645c284725e in decompileAction /home/tim/libming-asan/util/decompile.c:3465
#5 0x5645c284732e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
#6 0x5645c2840d13 in decompile_SWITCH /home/tim/libming-asan/util/decompile.c:2235
#7 0x5645c2842f7b in decompileIF /home/tim/libming-asan/util/decompile.c:2594
#8 0x5645c2846ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
#9 0x5645c284732e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
#10 0x5645c2847464 in decompile5Action /home/tim/libming-asan/util/decompile.c:3517
#11 0x5645c283348e in outputSWF_DOACTION /home/tim/libming-asan/util/outputscript.c:1551
#12 0x5645c2835a92 in outputBlock /home/tim/libming-asan/util/outputscript.c:2083
#13 0x5645c2836b88 in readMovie /home/tim/libming-asan/util/main.c:281
#14 0x5645c2837322 in main /home/tim/libming-asan/util/main.c:354
#15 0x7fbdee9fcb6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
#16 0x5645c2829469 in _start (/home/tim/libming-asan/util/.libs/swftocxx+0x14469)

0x61d0000008a8 is located 8 bytes to the right of 2080-byte region [0x61d000000080,0x61d0000008a0)
allocated by thread T0 here:
#0 0x7fbdee9f4f3e in calloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10c63e)
#1 0x5645c2842e26 in decompileIF /home/tim/libming-asan/util/decompile.c:2587
#2 0x5645c2846ea3 in decompileAction /home/tim/libming-asan/util/decompile.c:3335
#3 0x5645c284732e in decompileActions /home/tim/libming-asan/util/decompile.c:3494
#4 0x5645c2847464 in decompile5Action /home/tim/libming-asan/util/decompile.c:3517
#5 0x5645c283348e in outputSWF_DOACTION /home/tim/libming-asan/util/outputscript.c:1551
#6 0x5645c2835a92 in outputBlock /home/tim/libming-asan/util/outputscript.c:2083
#7 0x5645c2836b88 in readMovie /home/tim/libming-asan/util/main.c:281
#8 0x5645c2837322 in main /home/tim/libming-asan/util/main.c:354
#9 0x7fbdee9fcb6a 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:2473 in decompileIF
Shadow bytes around the buggy address:
 0x0c3a7fff80c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fff80d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fff80e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fff80f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3a7fff8100: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c3a7fff8110: 00 00 00 00 fa[fa]fa fa fa fa fa fa fa fa fa
 0x0c3a7fff8120: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c3a7fff8130: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c3a7fff8140: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c3a7fff8150: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c3a7fff8160: 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
==3097==ABORTING
```

  **cxizff** 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

