

New issue

[Jump to bottom](#)

heap overflow in decompile_SWITCH #191

[Open](#) cuanduo opened this issue on Jan 6, 2020 · 0 comments

cuanduo commented on Jan 6, 2020

```
export ASAN_OPTIONS=allocator_may_return_null=1
./swftopython $poc
segmentaion_fault_decompile_569-use_after_free-idx\0x1365-0x2.zip
```

asan output

```
root@ubuntu:/home/tim/libming/util# export ASAN_OPTIONS=allocator_may_return_null=1
root@ubuntu:/home/tim/libming/util# ../../asan/libming/util/swftopython overflows/segmentaion_fault_decompile_569-use_after_free-idx\0x1365-0x2
header indicates a filesize of 1484 but filesize is 228
#!/usr/bin/python
from ming import *

Ming_useSWFVersion(10);

m = SWFMovie();

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

# SWF_PLACEOBJECT3
Failed to find branch target!!!
Looking for: -2



==95555==WARNING: AddressSanitizer failed to allocate 0xfffffffffd438 bytes
Stream out of sync after parse of blocktype 12 (SWF_DOACTION). 223 but expecting 200.

# SWF_DOACTION
=====
==95555==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61e00000b28 at pc 0x55bee29d8d4c bp 0x7fff67e356e0 sp 0x7fff67e356d0
READ of size 8 at 0x61e00000b28 thread T0
#0 0x55bee29d8d4b in decompile_SWITCH /home/tim/asan/libming/util/decompile.c:2104
#1 0x55bee29dba67 in decompileIF /home/tim/asan/libming/util/decompile.c:2594
#2 0x55bee29df98f in decompileAction /home/tim/asan/libming/util/decompile.c:3335
#3 0x55bee29dfe1a in decompileActions /home/tim/asan/libming/util/decompile.c:3494
#4 0x55bee29df2da in decompileSETTARGET /home/tim/asan/libming/util/decompile.c:3169
#5 0x55bee29dfd4a in decompileAction /home/tim/asan/libming/util/decompile.c:3465
#6 0x55bee29dfe1a in decompileActions /home/tim/asan/libming/util/decompile.c:3494
#7 0x55bee29dff50 in decompile5Action /home/tim/asan/libming/util/decompile.c:3517
#8 0x55bee29cbfd8 in outputSWF_DOACTION /home/tim/asan/libming/util/outputscript.c:1551
#9 0x55bee29cf674 in readMovie /home/tim/asan/libming/util/main.c:281
#10 0x55bee29cf674 in readMovie /home/tim/asan/libming/util/main.c:281
#11 0x55bee29cf6e0 in main /home/tim/asan/libming/util/main.c:354
#12 0x7f3a8dc34b6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
#13 0x55bee29c2469 in _start (/home/tim/asan/libming/util/swftopython+0x14469)

0x61e00000b28 is located 8 bytes to the right of 2720-byte region [0x61e000000080,0x61e000000b20)
allocated by thread T0 here:
#0 0x7f3a8e06f63e in calloc (/lib/x86_64-linux-gnu/libasan.so.5+0x10c63e)
#1 0x55bee29db912 in decompileIF /home/tim/asan/libming/util/decompile.c:2587
#2 0x55bee29df98f in decompileAction /home/tim/asan/libming/util/decompile.c:3335
#3 0x55bee29dfe1a in decompileActions /home/tim/asan/libming/util/decompile.c:3494
#4 0x55bee29df2da in decompileSETTARGET /home/tim/asan/libming/util/decompile.c:3169
#5 0x55bee29dfd4a in decompileAction /home/tim/asan/libming/util/decompile.c:3465
#6 0x55bee29dfe1a in decompileActions /home/tim/asan/libming/util/decompile.c:3494
#7 0x55bee29dff50 in decompile5Action /home/tim/asan/libming/util/decompile.c:3517
#8 0x55bee29cbfd8 in outputSWF_DOACTION /home/tim/asan/libming/util/outputscript.c:1551
#9 0x55bee29cf674 in readMovie /home/tim/asan/libming/util/main.c:281
#10 0x55bee29cf674 in readMovie /home/tim/asan/libming/util/main.c:281
#11 0x55bee29cf6e0 in main /home/tim/asan/libming/util/main.c:354
#12 0x7f3a8dc34b6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/tim/asan/libming/util/decompile.c:2104 in decompile_SWITCH
Shadow bytes around the buggy address:
 0x0c3c7fff8110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3c7fff8120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3c7fff8130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3c7fff8140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c3c7fff8150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c3c7fff8160: 00 00 00 00 fa[fa]fa fa fa fa fa fa fa fa fa
0x0c3c7fff8170: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3c7fff8180: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3c7fff8190: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3c7fff81a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c3c7fff81b0: 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
==95555==ABORTING
root@ubuntu:/home/tim/libming/util#
```

  **cx1zff** 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

