New issue

Jump to bottom

null pointer reference in decompileGETURL2 #190

Open **cuanduo** opened this issue on Jan 6, 2020 · 0 comments

cuanduo commented on Jan 6, 2020

swftophp $poc

libming_decompile762poc-out_of_mem-idx:0xfcd-0x0.zip

asan output

```
root@ubuntu:/home/tim/libming/util# ../../asan/libming/util/swftophp overflows/libming_decompile762poc-out_of_mem-idx\:0xfcd-0x0
header indicates a filesize of 36374837 but filesize is 58
<?php
$m = new SWFMovie(8);

ming_setscale(1.0);
$m->setRate(3.925781);
$m->setDimension(0, 0);

/* Note: xMin and/or yMin are not 0! */

$m->setFrames(4079);

/* SWF_DOACTION */
AddressSanitizer:DEADLYSIGNAL
=================================================================
==2294==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x559547345499 bp 0x7fff7c524450 sp 0x7fff7c524420 T0)
==2294==The signal is caused by a READ memory access.
==2294==Hint: address points to the zero page.
    #0 0x559547345498 in decompileGETURL2 /home/tim/asan/libming/util/decompile.c:924
    #1 0x559547350708 in decompileAction /home/tim/asan/libming/util/decompile.c:3236
    #2 0x559547350ed6 in decompileActions /home/tim/asan/libming/util/decompile.c:3494
    #3 0x55954735100c in decompile5Action /home/tim/asan/libming/util/decompile.c:3517
    #4 0x55954733d007 in outputSWF_DOACTION /home/tim/asan/libming/util/outputscript.c:1551
    #5 0x55954733f63a in outputBlock /home/tim/asan/libming/util/outputscript.c:2083
    #6 0x559547340730 in readMovie /home/tim/asan/libming/util/main.c:281
    #7 0x559547340eca in main /home/tim/asan/libming/util/main.c:354
    #8 0x7fba80753b6a in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x26b6a)
    #9 0x559547333469 in _start (/home/tim/asan/libming/util/swftophp+0x14469)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/tim/asan/libming/util/decompile.c:924 in decompileGETURL2
==2294==ABORTING
root@ubuntu:/home/tim/libming/util# vim
```

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