New issue

Jump to bottom

Segmentation fault in function getName, decompile.c:457 #201

○ Open 5hadowblad3 opened this issue on Aug 24, 2020 · 0 comments

5hadowblad3 commented on Aug 24, 2020

Hi, there.

There is a segmentation fault in the newest master branch `04aee52` .
Here is the reproducing command:

```
swftophp poc
```

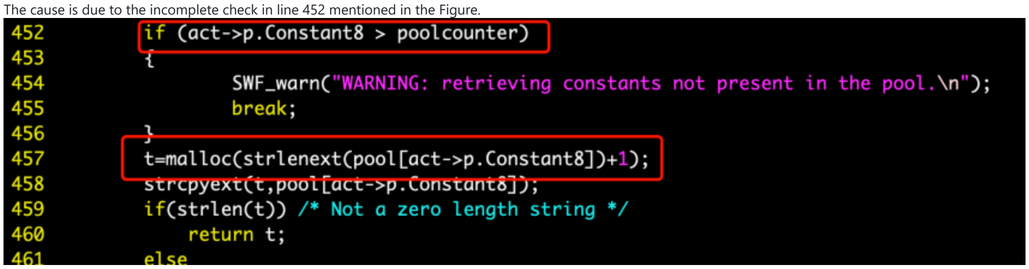
POC:
seg-decompile457.zip

Here is the reproduce trace reported by ASAN:

```
==19422==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000041ef74 bp 0x0c10000017fb sp 0x7ffee6469480 T0)
    #0 0x41ef73 in getName ../../util/decompile.c:457
    #1 0x42b65b in decompileDELETE ../../util/decompile.c:3175
    #2 0x42b65b in decompileAction ../../util/decompile.c:3436
    #3 0x44e234 in decompileActions ../../util/decompile.c:3535
    #4 0x44e234 in decompile5Action ../../util/decompile.c:3558
    #5 0x4114d9 in outputSWF_INITACTION ../../util/outputscript.c:1860
    #6 0x402836 in readMovie ../../util/main.c:281
    #7 0x402836 in main ../../util/main.c:354
    #8 0x7f82c681082f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #9 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../../util/decompile.c:457 getName
==19422==ABORTING
```

The cause is due to the incomplete check in line 452 mentioned in the Figure.



```
452         if (act->p.Constant8 > poolcounter)
453         {
454                 SWF_warn("WARNING: retrieving constants not present in the pool.\n");
455                 break;
456         }
457         t=malloc(strlenext(pool[act->p.Constant8])+1);
458         strcpyext(t,pool[act->p.Constant8]);
459         if(strlen(t)) /* Not a zero length string */
460             return t;
461         else
```

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