

New issue

[Jump to bottom](#)

## Segmentation fault in function getString, decompile.c:380 #202

[Open](#) Shadowblad3 opened this issue on Aug 24, 2020 · 1 comment

Shadowblad3 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-decompile380.zip](#)

Here is the reproduce trace reported by ASAN:

```
==187067==ERROR: AddressSanitizer: SEGV on unknown address 0x000000000000 (pc 0x00000041d8dc bp 0x00000003f178 sp 0x7ffe801f8bb0 T0)
#0 0x41d8db in getString ../../util/decompile.c:380
#1 0x424764 in decompilePUSHPARAM ../../util/decompile.c:878
#2 0x42d225 in decompileSTARTDRAG ../../util/decompile.c:3054
#3 0x42d225 in decompileAction ../../util/decompile.c:3433
#4 0x44e234 in decompileActions ../../util/decompile.c:3535
#5 0x44e234 in decompileSAction ../../util/decompile.c:3558
#6 0x4114d9 in outputSWF_INITACTION ../../util/outputscript.c:1860
#7 0x402836 in readMovie ../../util/main.c:281
#8 0x402836 in main ../../util/main.c:354
#9 0x7fe9f9c4482f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#10 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../../util/decompile.c:380 getString
==187067==ABORTING
```

The cause is due to the unchecked index of act-&gt;p.Constant8 mentioned in Figure.

```
374     case PUSH_CONSTANT: /* CONSTANT8 */
375         if (act->p.Constant8 > poolcounter)
376         {
377             SWF_warn("WARNING: retrieving constants not present in the pool.\n");
378             break;
379         }
380         t=malloc(strlenext(pool[act->p.Constant8])+3); /* 2 ""'s and a NULL */
381         strcpy(t, "");
382         strcatext(t, pool[act->p.Constant8]);
383         strcat(t, "");
384         return t;
385     case PUSH_CONSTANT16: /* CONSTANT16 */
```

Shadowblad3 commented on Aug 24, 2020

Author

another related traces:

```
==79447==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60300000eeab at pc 0x00000041fa80 bp 0x7ffc68aab490 sp 0x7ffc68aab480
WRITE of size 1 at 0x60300000eeab thread T0
#0 0x41fa7f in strcpyext ../../util/decompile.c:259
#1 0x41fa7f in getName ../../util/decompile.c:435
#2 0x4304b8 in decompileREMOVECLIP ../../util/decompile.c:3108
#3 0x4304b8 in decompileAction ../../util/decompile.c:3497
#4 0x44e234 in decompileActions ../../util/decompile.c:3535
#5 0x44e234 in decompileSAction ../../util/decompile.c:3558
#6 0x4114d9 in outputSWF_INITACTION ../../util/outputscript.c:1860
#7 0x402836 in readMovie ../../util/main.c:281
#8 0x402836 in main ../../util/main.c:354
#9 0x7fcebce0482f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#10 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)



0x60300000eeab is located 0 bytes to the right of 27-byte region [0x60300000ee90,0x60300000eeab)
allocated by thread T0 here:
#0 0x7fcebdc59662 in malloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x98662)
#1 0x41f3d0 in getName ../../util/decompile.c:434

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../util/decompile.c:259 strcpyext
Shadow bytes around the buggy address:
 0x0c067fff9d80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9d90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9da0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9db0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9dc0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
->0x0c067fff9dd0: fa fa 00 00 00[03]fa fa 00 00 00 fa fa 00 00
 0x0c067fff9de0: 00 fa fa fa 00 00 00 fa fa 00 00 00 fa fa
 0x0c067fff9df0: 00 00 00 fa fa 00 00 00 fa fa fd fd fd
 0x0c067fff9e00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9e10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c067fff9e20: 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
Heap right redzone: fb
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack partial redzone: f4
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

==79447==ABORTING
```

  **cxlzzf** 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

