New issue

Jump to bottom

Buffer overflow in decompileIF, decompile.c:2516 #204

Open **5hadowblad3** opened this issue on Aug 25, 2020 · 0 comments

5hadowblad3 commented on Aug 25, 2020

Hi, there.

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

```
swftophp poc
```

POC:
overflow-decompiler2516.zip

Here is the reproduce trace reported by ASAN:

```
==165852==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60e00000dc88 at pc 0x00000044d878 bp 0x7ffd6043c430 sp 0x7ffd6043c420
READ of size 8 at 0x60e00000dc88 thread T0
    #0 0x44d877 in decompileIF ../../util/decompile.c:2516
    #1 0x442c5c in decompileActions ../../util/decompile.c:3535
    #2 0x442c5c in decompileIF ../../util/decompile.c:2407
    #3 0x43d3d4 in decompileActions ../../util/decompile.c:3535
    #4 0x43d3d4 in decompileSETTARGET ../../util/decompile.c:3211
    #5 0x43c38b in decompileActions ../../util/decompile.c:3535
    #6 0x432866 in decompileTRY ../../util/decompile.c:2785
    #7 0x432866 in decompileAction ../../util/decompile.c:3518
    #8 0x44e234 in decompileActions ../../util/decompile.c:3535
    #9 0x44e234 in decompileSAction ../../util/decompile.c:3558
    #10 0x411304 in outputSWF_DOACTION ../../util/outputscript.c:1551
    #11 0x402836 in readMovie ../../util/main.c:281
    #12 0x402836 in main ../../util/main.c:354
    #13 0x7f8b968e382f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
    #14 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)

0x60e00000dc88 is located 8 bytes to the right of 160-byte region [0x60e00000dbe0,0x60e00000dc80)
allocated by thread T0 here:
    #0 0x7f8b972487fa in __interceptor_calloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x987fa)
    #1 0x45e4cc in parseSWF_ACTIONRECORD ../../util/parser.c:1062

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../util/decompile.c:2516 decompileIF
Shadow bytes around the buggy address:
  0x0c1c7fff9b40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9b50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9b60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c1c7fff9b70: fa fa fa fa fa fa fa fa fa fa fa fa 00 00 00 00
  0x0c1c7fff9b80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c1c7fff9b90: fa[fa]fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c1c7fff9ba0: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c1c7fff9bb0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c1c7fff9bc0: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c1c7fff9bd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c1c7fff9be0: 00 00 00 00 fa fa fa fa fa fa fa fa fd fd fd fd
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
==165852==ABORTING
```

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