

New issue

Jump to bottom

Buffer overflow in newVar_N, decompile.c:751 #205

Open Shadowblad3 opened this issue on Aug 25, 2020 · 0 comments

Shadowblad3 commented on Aug 25, 2020

Hi, there.

There is a buffer overflow in the newest master branch [04aee52](#) which causes a huge memory information leakage.
Here is the reproducing command:

```
swftophp poc
```

POC:


[overflow-decompiler751.zip](#)

Here is the reproduce trace reported by ASAN:

```
==8303==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000026680 at pc 0x7f2f1360124b bp 0x7ffc9987390 sp 0x7ffc9986b38
READ of size 1025 at 0x619000026680 thread T0
#0 0x7f2f1360124a in strlen (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x7024a)
#1 0x425b98 in newVar_N ../../util/decompile.c:751
#2 0x435db7 in decompileNEWOBJECT ../../util/decompile.c:1720
#3 0x435db7 in decompileAction ../../util/decompile.c:3324
#4 0x43d3d4 in decompileActions ../../util/decompile.c:3535
#5 0x43d3d4 in decompileSETTARGET ../../util/decompile.c:3211
#6 0x43c38b in decompileActions ../../util/decompile.c:3535
#7 0x432866 in decompileTRY ../../util/decompile.c:2785
#8 0x432866 in decompileAction ../../util/decompile.c:3518
#9 0x44e234 in decompileActions ../../util/decompile.c:3535
#10 0x44e234 in decompile5Action ../../util/decompile.c:3558
#11 0x411304 in outputSWF_DOACTION ../../util/outputscript.c:1551
#12 0x402836 in readMovie ../../util/main.c:281
#13 0x402836 in main ../../util/main.c:354
#14 0x7f2f12cc482f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#15 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)

0x619000026680 is located 0 bytes to the right of 1024-byte region [0x619000026280,0x619000026680)
allocated by thread T0 here:
#0 0x7f2f136299c1 in realloc (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x989c1)
#1 0x425b7b in newVar_N ../../util/decompile.c:754

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../util/decompile.c:751
Shadow bytes around the buggy address:
 0x0c327fffcc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fffcc90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fffcca0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fffccb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c327fffccd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fffccd0:[fa]fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fffcd10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c327fffcd20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c327fffcd30: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c327fffcd40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
 0x0c327fffcd50: fd fd fd fd fd fd fd fd fd fd fd fd 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
==8303==ABORTING
```

 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

