

[New issue](#)[Jump to bottom](#)

Segmentation fault in function decompileINCR_DECR, decompile.c 1640 #203

[Open](#) Shadowblad3 opened this issue on Aug 25, 2020 · 0 comments

Shadowblad3 commented on Aug 25, 2020

Hi, there.

There is a segmentation fault in the newest master branch [04aee52](#) .
Here is the reproducing command:

swftophp poc

POC:

[seg-decompile1640.zip](#)


Here is the reproduce trace reported by ASAN:

```
==79767==ERROR: AddressSanitizer: SEGV on unknown address 0x00000000010 (pc 0x00000042782c bp 0x0000000000f0 sp 0x7ffdbd64ccf0 T0)
#0 0x42782b in decompileINCR_DECR ../../util/decompile.c:1640
#1 0x44e234 in decompileActions ../../util/decompile.c:3535
#2 0x44e234 in decompileSAction ../../util/decompile.c:3558
#3 0x4114d9 in outputSWF_INITACTION ../../util/outputscript.c:1860
#4 0x402836 in readMovie ../../util/main.c:281
#5 0x402836 in main ../../util/main.c:354
#6 0x7fd557eb582f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2082f)
#7 0x403b38 in _start (/mnt/data/playground/libming/build/util/swftophp+0x403b38)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV ../../util/decompile.c:1640 decompileINCR_DECR
==79767==ABORTING
```

The cause might due to the incomplete check related to the index for array regs.

```
1634         push(var);
1635     }
1636     else
1637     {
1638         if(OpCode(actions, n-1, maxn) == SWFACTION_PUSH &&
1639            OpCode(actions, n+1, maxn) == SWFACTION_STOREREGISTER &&
1640            regs[actions[n+1].SWF_ACTIONSTOREREGISTER.Register]->Type == PUSH_VARIABLE)
1641         {
1642             var = newVar2(dblp, getString(var));
1643             if ((OpCode(actions, n+2, maxn) == SWFACTION_POP
1644                  && actions[n-1].SWF_ACTIONPUSH.NumParam==1)
1645                 || OpCode(actions, n+3, maxn) == SWFACTION_POP)
1646             {
```

 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

