

```
==17764==ERROR: AddressSanitizer: global-buffer-overflow on address 0x00000102f062 at pc
0x00000051d4ce bp 0x7ffdfad96390 sp 0x7ffdfad96388
WRITE of size 2 at 0x00000102f062 thread T0
    #0 0x51d4cd in compilePassOpcode
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:1896:31
    #1 0x50f7bf in compileRule
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:3947:11
    #2 0x4ff42b in compileFile
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:4660:9
    #3 0x4fbbe9 in compileTable
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:4767:9
    #4 0x4f9bdf in getTable
```

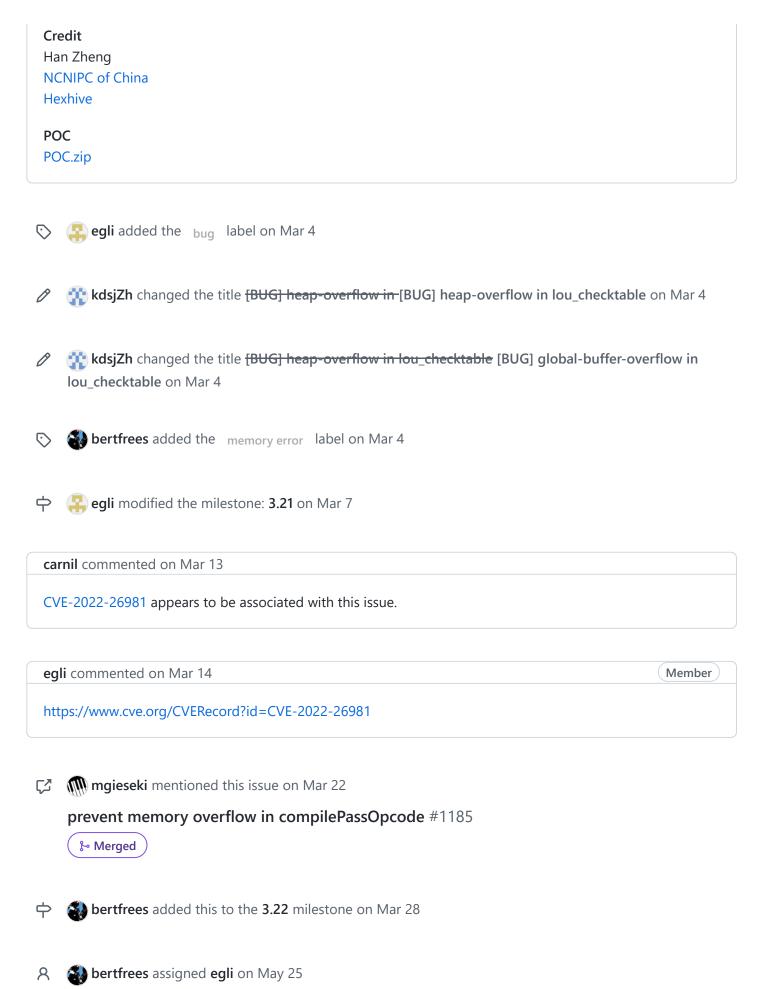
```
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:4939:7
  #5 0x4f9061 in lou getTable
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:4848:2
  #6 0x4fb51f in lou getTable
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:4860:2
  #7 0x4f4109 in main /benchmark/vulnerable/liblouis/tools/lou_checktable.c:114:16
  #8 0x7f6ff64f0bf6 in libc start main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-
start.c:310
  #9 0x41b699 in _start (/benchmark/vulnerable/liblouis/tools/lou_checktable+0x41b699)
0x00000102f062 is located 0 bytes to the right of global variable 'passRuleDots' defined in
'compileTranslationTable.c:1850:21' (0x102e060) of size 4098
SUMMARY: AddressSanitizer: global-buffer-overflow
/benchmark/vulnerable/liblouis/liblouis/compileTranslationTable.c:1896:31 in compilePassOpcode
Shadow bytes around the buggy address:
 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
 Freed heap region:
 Stack left redzone:
                 f1
 Stack mid redzone:
                f2
 Stack right redzone:
                f3
 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:
 Intra object redzone:
 ASan internal:
                 fe
 Left alloca redzone:
                 ca
 Right alloca redzone:
                 cb
 Shadow gap:
                 CC
==17764==ABORTING
```

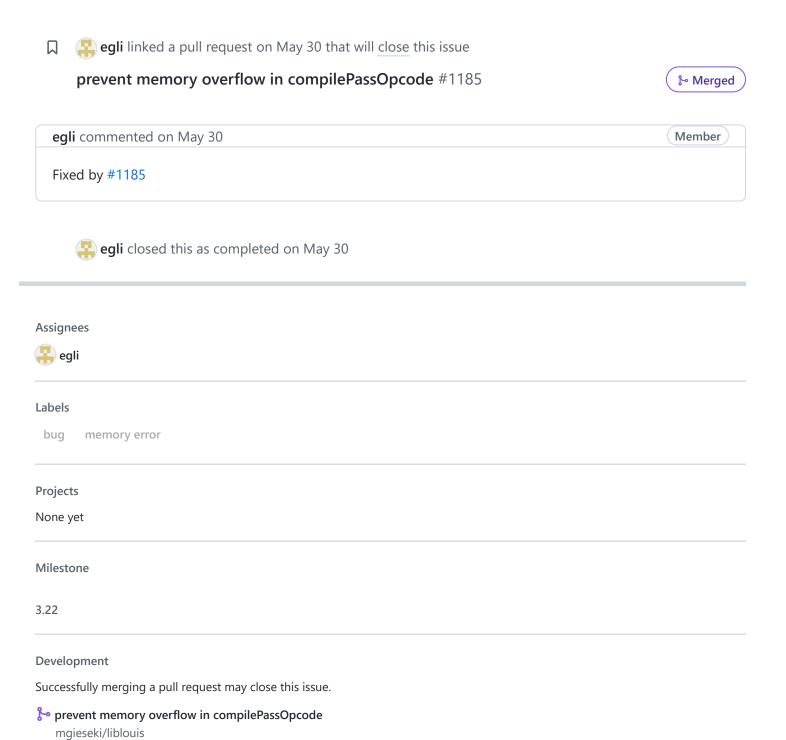
System

OS: Ubuntu

OS version: can be reproduced in 18.04/20.04

clang version: 12.0.1 (release/12.x) liblouis Version: latest commit 4d73c81





4 participants







