

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

[BUG] global-buffer-overflow in lou_checktable #1171

Closed

kdsjZh opened this issue on Mar 4 · 3 comments · Fixed by #1185

Assignees



Labels

bug memory error

Milestone

3.22

kdsjZh commented on Mar 4 • edited ▾

Describe the bug

There is a global-buffer-overflow bug found in compilePassOpcode, can be triggered via lou_checktable+ASan

To Reproduce

Steps to reproduce the behavior:

```
export CC=clang && export CFLAGS="-fsanitize=address -g"  
./autogen.sh && ./configure --disable-shared --disable-local-libopts && make clean && make -j8  
./tools/lou_checktable POC
```

Output:

```
==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:
  0x0000801fddb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fddc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fddd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fdde0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801fddf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0000801fde00: 00 00 00 00 00 00 00 00 00 00 00 00[02]f9 f9 f9
  0x0000801fde10: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fde20: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fde30: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fde40: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
  0x0000801fde50: f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9 f9
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:    fd
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:         ac
Intra object redzone: bb
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](#)

Credit

Han Zheng

[NCNIPC of China](#)

[Hexhive](#)

POC



[POC.zip](#)

  **egli** added the `bug` label on Mar 4

  **kdsjZh** changed the title ~~[BUG] heap-overflow in~~ **[BUG] heap-overflow in lou_checktable** on Mar 4

  **kdsjZh** changed the title ~~[BUG] heap-overflow in lou_checktable~~ **[BUG] global-buffer-overflow in lou_checktable** on Mar 4

  **bertfrees** added the `memory error` label on Mar 4

  **egli** modified the milestone: **3.21** on Mar 7

carnil commented on Mar 13

[CVE-2022-26981](#) appears to be associated with this issue.

egli commented on Mar 14

Member

<https://www.cve.org/CVERecord?id=CVE-2022-26981>


  **mgieseki** mentioned this issue on Mar 22

prevent memory overflow in compilePassOpcode #1185

 Merged

  **bertfrees** added this to the **3.22** milestone on Mar 28

  **bertfrees** assigned **egli** on May 25

🔖  egli linked a pull request on May 30 that will close this issue

prevent memory overflow in compilePassOpcode #1185

 Merged

egli commented on May 30

Member

Fixed by [#1185](#)

 egli closed this as completed on May 30

Assignees

 egli

Labels

bug memory error

Projects


None yet

Milestone

3.22

Development

Successfully merging a pull request may close this issue.

 **prevent memory overflow in compilePassOpcode**
mgieseki/liblouis

4 participants

