liblouis / **liblouis** Public

Code   Issues 191   Pull requests 12   Actions   Projects   Wiki   ...

New issue

Jump to bottom

[BUG] invalid memory writes in compileRule, liblouis/compileTranslationTable.c:3744 #1214

Closed   **kdsjZh** opened this issue on May 21 · 4 comments · Fixed by #1217

Assignees

Labels   memory error

Milestone   3.22

kdsjZh commented on May 21 • edited

summary

Hello, I was testing my new fuzzer and found an invalid memory write in function compileRule, liblouis/compileTranslationTable.c:3744. Which can be triggered via lou_trace + ASan.

step to reproduce

```
export CFLAGS="-fsanitize=address -g"
./autogen.sh && ./configure  && make -j8
./tools/lou_trace  $POC
```

Environment

- ubuntu 22.04 (docker image),
- gcc 11.2.0
- liblouis latest commit `83c9135`

ASAN report

```
poc1:24: warning: invalid UTF-8. Assuming Latin-1.
...
poc1:145: error: invalid 4-digit hexadecimal number
AddressSanitizer:DEADLYSIGNAL
=================================================================
==3739596==ERROR: AddressSanitizer: SEGV on unknown address 0x630000015722 (pc 0x7f3962ff103a bp
0x7ffcbf6d48b0 sp 0x7ffcbf6c2180 T0)
==3739596==The signal is caused by a WRITE memory access.
    #0 0x7f3962ff103a in compileRule /benchmark/liblouis/liblouis/compileTranslationTable.c:3744
    #1 0x7f3962ff863a in compileFile /benchmark/liblouis/liblouis/compileTranslationTable.c:4660
    #2 0x7f3962ff92b3 in compileTable /benchmark/liblouis/liblouis/compileTranslationTable.c:4777
    #3 0x7f3962ffa6f2 in getTable /benchmark/liblouis/liblouis/compileTranslationTable.c:4949
    #4 0x7f3962ff99b4 in _lou_getTable /benchmark/liblouis/liblouis/compileTranslationTable.c:4858
    #5 0x7f3962ff9bf6 in lou_getTable /benchmark/liblouis/liblouis/compileTranslationTable.c:4870
    #6 0x55643186bfb5 in main /benchmark/liblouis/tools/lou_trace.c:392
    #7 0x7f3962dc3d8f in __libc_start_call_main ../sysdeps/nptl/libc_start_call_main.h:58
    #8 0x7f3962dc3e3f in __libc_start_main_impl ../csu/libc-start.c:392
    #9 0x556431868644 in _start (/benchmark/liblouis/tools/.libs/lou_trace+0x3644)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /benchmark/liblouis/liblouis/compileTranslationTable.c:3744 in
compileRule
==3739596==ABORTING
```

Credit

Han Zheng
NCNIPC of China
Hexhive

POC

poc1.zip

bertfrees added the memory error label on May 25

egli added this to the **3.22** milestone on May 25

bertfrees assigned **egli** on May 25

egli added a commit that referenced this issue on May 25

`Prevent an invalid memory writes in compileRule` … `ff747ec`

✓

egli mentioned this issue on May 25

Prevent an invalid memory writes in compileRule #1217

Merged

kdsjZh commented on May 26 Author

Just verified and in my environment it's fixed now. Thanks!

kdsjZh closed this as completed on May 26

bertfrees commented on May 26 Member

Reopening as #1217 is not merged yet.

kdsjZh reopened this on May 27

egli added a commit that referenced this issue on May 30

```
Prevent an invalid memory writes in compileRule  …          ✓ 2e4772b
```

egli closed this as completed in #1217 on May 30

risicle commented on Jun 20 Contributor

Did this get a CVE assigned to it? Looks like it should.

kdsjZh commented on Jun 21 Author

Yes, CVE-2022-31783.

Assignees

egli

Labels

memory error

Projects

None yet

Milestone

3.22

Development

Successfully merging a pull request may close this issue.

Prevent an invalid memory writes in compileRule
liblouis/liblouis

4 participants