Juniper / **libslax** Public

Code   Issues 28   Pull requests 5   Actions   Projects   Wiki   ···

New issue

Jump to bottom

A dynamic-stack-buffer-overflow in slaxlexer.c:955:4 #53

Open **seviezhou** opened this issue on Aug 3, 2020 · 0 comments

seviezhou commented on Aug 3, 2020

System info

Ubuntu X64, gcc (Ubuntu 5.5.0-12ubuntu1), slaxproc (latest master 45d88a)

Configure

CFLAGS="-g -fsanitize=address" LDFLAGS="-fsanitize=address" ./configure

Command line

./build/slaxproc/slaxproc -o /dev/null -x @@

AddressSanitizer output

```
=================================================================
==36347==ERROR: AddressSanitizer: dynamic-stack-buffer-overflow on address 0x7fff6881f323 at pc 0x0000004e0985 bp 0x7fff6881f2f0 sp 0x7fff6881eaa0
WRITE of size 4 at 0x7fff6881f323 thread T0
    #0 0x4e0984 in __asan_memcpy /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:23
    #1 0x5612b4 in slaxLexer /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:955:4
    #2 0x55f3a5 in slaxYylex /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:1272:10
    #3 0x579c59 in slaxParse /home/seviezhou/libslax/build/libslax/slaxparser.c:2447:16
    #4 0x56df6e in slaxLoadFile /home/seviezhou/libslax/build/libslax/../../libslax/slaxloader.c:731:10
    #5 0x524b1e in do_slax_to_xslt /home/seviezhou/libslax/build/slaxproc/../../slaxproc/slaxproc.c:156:9
    #6 0x51f1d8 in main /home/seviezhou/libslax/build/slaxproc/../../slaxproc/slaxproc.c:1039:5
    #7 0x7f7f0fd7883f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
    #8 0x41d818 in _start (/home/seviezhou/libslax/build/slaxproc/slaxproc+0x41d818)

Address 0x7fff6881f323 is located in stack of thread T0
SUMMARY: AddressSanitizer: dynamic-stack-buffer-overflow /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_interceptors_memintrinsics.cc:23 in __asan_memcpy
Shadow bytes around the buggy address:
  0x10006d0fbe10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10006d0fbe60: ca ca ca ca[03]cb cb cb cb cb cb cb 00 00 00 00
  0x10006d0fbe70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbe90: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10006d0fbea0: f1 f1 f1 f1 00 f2 f2 f2 00 00 00 00 00 00 00 00
  0x10006d0fbeb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==36347==ABORTING
```

POC

dynamic-stack-overflow-slaxLexer-slaxlexer-955.zip

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant