

New issue

Jump to bottom

# A heap-buffer-overflow in slaxlexer.c:986:11 #51

Open seviezhou opened this issue on Aug 2, 2020 · 0 comments

Assignees



seviezhou commented on Aug 2, 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

```
=====
==54185==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x625000002100 at pc 0x0000005661fa bp 0x7fff21d66b10 sp 0x7fff21d66b08
READ of size 1 at 0x625000002100 thread T0
#0 0x5661f9 in slaxLexer /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:986:11
#1 0x55f3a5 in slaxVylex /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:1272:10
#2 0x579c59 in slaxParse /home/seviezhou/libslax/build/libslax/slaxparser.c:2447:16
#3 0x56df6e in slaxLoadFile /home/seviezhou/libslax/build/libslax/../../libslax/slaxloader.c:731:10
#4 0x524b1e in do_slax_to_xslt /home/seviezhou/libslax/build/slaxproc/../../slaxproc/slaxproc.c:156:9
#5 0x51f1d8 in main /home/seviezhou/libslax/build/slaxproc/../../slaxproc/slaxproc.c:1039:5
#6 0x7f8c06e7f83f in __libc_start_main /build/glibc-e6zv40/glibc-2.23/csu/../csu/libc-start.c:291
#7 0x41d818 in _start (/home/seviezhou/libslax/build/slaxproc/slaxproc+0x41d818)

0x625000002100 is located 0 bytes to the right of 8192-byte region [0x625000000100,0x625000002100)
allocated by thread T0 here:
#0 0x4e1e90 in realloc /home/seviezhou/llvm-6.0.0/projects/compiler-rt/lib/asan/asan_malloc_linux.cc:107
#1 0x55da4f3 in slaxGetInput /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:601:14

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:986:11 in slaxLexer
Shadow bytes around the buggy address:
 0x0c4a7fff83d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c4a7fff83e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c4a7fff83f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c4a7fff8400: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 0x0c4a7fff8410: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
->0x0c4a7fff8420:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c4a7fff8430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c4a7fff8440: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c4a7fff8450: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c4a7fff8460: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
 0x0c4a7fff8470: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==54185==ABORTING
```

## POC

heap-overflow-slaxLexer-slaxlexer-986.zip

philshafer self-assigned this on Aug 3, 2020

Assignees



Labels

None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests
2 participants
 