New issue

A heap-buffer-overflow in slaxlexer.c:751:13 #52



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

```
==59937==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x625000002100 at pc 0x0000005671b1 bp 0x7fff6c8e6110 sp 0x7fff6c8e6108
READ of size 1 at 0x625000002100 thread T0
```

#0 0x5671b0 in slaxIsCommentStart /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:751:13

#1 0x5671b0 in slaxLexer /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:919

#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

#8 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

 $\verb|#1 0x55daf3 in slaxGetInput /home/seviezhou/libslax/build/libslax/.../../libslax/slaxlexer.c: 601:14 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 | 1.0 |$

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/seviezhou/libslax/build/libslax/../../libslax/slaxlexer.c:751:13 in slaxIsCommentStart

Addressable: Partially addressable: 01 02 03 04 05 06 07

Heap left redzone: Freed heap region: Stack left redzone:

Stack mid redzone: Stack right redzone:

Stack after return:

Stack use after scope:

Global redzone:

Global init order:

Poisoned by user: Container overflow:

Array cookie: Intra object redzone:

ASan internal:

Left alloca redzone: Right alloca redzone:

==59937==ABORTING

POC

heap-overflow-slaxlsCommentStart-slaxlexer-751.zip

A philshafer self-assigned this on Aug 3, 2020



Jump to bottom

abels None yet
Projects None yet
dilestone No milestone
Development No branches or pull requests

2 participants

