New issue

Jump to bottom

A heap-buffer-overflow in asn_compiler.hpp:11676 #30

Open seviezhou opened this issue on Aug 7, 2020 · 3 comments

seviezhou commented on Aug 7, 2020

System info

Ubuntu x86_64, gcc, fast_ber_compiler (latest master 7262b5)

Configure

cmake .. -DCMAKE_CXX_FLAGS="-fsanitize=address -g" -DCMAKE_C_FLAGS="-fsanitize=address -g" -DCMAKE_EXE_LINKER_FLAGS="-fsanitize=address"

Command line

./build_cmake/src/fast_ber_compiler @@ /tmp/fastber

AddressSanitizer output

```
=================================================================
==15839==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61500000fee1 at pc 0x0000004cd964 bp 0x7ffc3afd8830 sp 0x7ffc3afd8820
READ of size 1 at 0x61500000fee1 thread T0
    #0 0x4cd963 in yy::yylex(Context&) /home/styler/git/fast_ber/build_debug/src/autogen/asn_compiler.hpp:11676
    #1 0x4ecd8b in yy::asn1_parser::parse() /home/styler/git/fast_ber/build_debug/src/autogen/asn_compiler.re:7571
    #2 0x45eb31 in main /home/seviezhou/fastber/src/compiler_main/CompilerMain.cpp:481
    #3 0x7f68aedde83f in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x2083f)
    #4 0x469968 in _start (/home/seviezhou/fastber/build_cmake/src/fast_ber_compiler+0x469968)

0x61500000fee1 is located 0 bytes to the right of 481-byte region [0x61500000fd00,0x61500000fee1)
allocated by thread T0 here:
    #0 0x7f68afd42532 in operator new(unsigned long) (/usr/lib/x86_64-linux-gnu/libasan.so.2+0x99532)
    #1 0x5829dd in void std::__cxx11::basic_string<char, std::char_traits<char>, std::allocator<char> >::_M_construct<std::istreambuf_iterator<char, std::char_traits<char> > >
(std::istreambuf_iterator<char, std::char_traits<char> >, std::istreambuf_iterator<char, std::char_traits<char> >, std::input_iterator_tag)
/usr/include/c++/5/bits/basic_string.tcc:188

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/styler/git/fast_ber/build_debug/src/autogen/asn_compiler.hpp:11676 yy::yylex(Context&)
Shadow bytes around the buggy address:
  0x0c2a7fff9f80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff9f90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff9fa0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff9fb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2a7fff9fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c2a7fff9fd0: 00 00 00 00 00 00 00 00 00 00 00[01]fa fa fa
  0x0c2a7fff9fe0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fff9ff0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffa000: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffa010: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a7fffa020: 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
  Heap right redzone:      fb
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack partial redzone:   f4
  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
==15839==ABORTING
```

POC

heap-overflow-yylex-asn_compiler-11676.zip

Samuel-Tyler commented on Aug 7, 2020 Owner

Thankyou, I will investigate. I assume this issue is intentional to reproduce the bug;

```
Pokemon"DEFINITIONS
```

seviezhou commented on Aug 7, 2020 Author

Actually, I am performing fuzzing on the compiler.

I'm not sure if you think it is necessary to generate random data to test the compiler.

Samuel-Tyler commented on Aug 7, 2020 Owner

I see, I appreciate your efforts. It is interesting to see.

I would not be surprised if there are many issues as robustness of the compiler has not been tested much.

 **slandelle** mentioned this issue on Apr 30, 2021

CVE-2020-23921 vulnerability reported on fast-uuid jchambers/fast-uuid#14

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants