# Heap-buffer-overflow in jsonlint/src/lexer.cpp:18:15 #2

Open **yangfar** opened this issue on Oct 1 · 0 comments

**yangfar** commented on Oct 1

Hi, developers of jsonlint.
I fuzz the jsonlint with AFL,and some crashes incurred—heap-buffer-overflow.The following is the details.
**Commond: ./jsonlint input**

## Bug

```
=1492403==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60e0000000df at pc
0x000000508ea7 bp 0x7ffc32b00ef0 sp 0x7ffc32b00ee8
READ of size 1 at 0x60e0000000df thread T0
#0 0x508ea6 in jsonlint::details::ReadCharacter[abi:cxx11](jsonlint::Lexer&, bool)
/home/hjsz/jsonlint/src/lexer.cpp:18:15
#1 0x509c58 in jsonlint::details::PeekCharacterabi:cxx11 /home/hjsz/jsonlint/src/lexer.cpp:27:52
#2 0x509c58 in jsonlint::details::ReadString(jsonlint::Lexer&) /home/hjsz/jsonlint/src/lexer.cpp:48:12
#3 0x512b99 in jsonlint::Tokenize(jsonlint::Lexer&) /home/hjsz/jsonlint/src/lexer.cpp:256:26
#4 0x4cb5b1 in main /home/hjsz/jsonlint/src/main.cpp:26:21
#5 0x7f1da2c68082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
#6 0x41fced in _start (/home/hjsz/jsonlint/build/jsonlint+0x41fced)

0x60e0000000df is located 0 bytes to the right of 159-byte region [0x60e000000040,0x60e0000000df)
allocated by thread T0 here:
#0 0x4c7b9d in operator new(unsigned long) (/home/hjsz/jsonlint/build/jsonlint+0x4c7b9d)
#1 0x52d49c in void std::__cxx11::basic_string<char, std::char_traits, std::allocator >::_M_construct<char*>
(char*, char*, std::forward_iterator_tag) /usr/bin/../lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/basic_string.tcc:219:14
#2 0x4cb40f in main /home/hjsz/jsonlint/src/main.cpp:25:19
#3 0x7f1da2c68082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
```

```
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/hjsz/jsonlint/src/lexer.cpp:18:15 in
jsonlint::details::ReadCharacter[abi:cxx11](jsonlint::Lexer&, bool)
Shadow bytes around the buggy address:
0x0c1c7fff7fc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c1c7fff7fd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c1c7fff7fe0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c1c7fff7ff0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c1c7fff8000: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
=>0x0c1c7fff8010: 00 00 00 00 00 00 00 00 00 00 00[07]fa fa fa fa
0x0c1c7fff8020: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1c7fff8030: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1c7fff8040: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1c7fff8050: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1c7fff8060: 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
Shadow gap: cc
==1492403==ABORTING
```

## Crashes

crashes.zip

## Environment

Ubuntu 20.04.5 LTS
master

Thanks for your time.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant