Some crashes occur when fuzzing rtf2html. #11

Open **yangfar** opened this issue on Oct 9 · 0 comments

yangfar commented on Oct 9

Version

hjsz@hjsz:~/rtf2html$ ./rtf2html -v
rtf2html version 0.2.0

Command

./rtf2html

Crash output

Crash1: heap-buffer-overflow

```
=================================================================
==3467450==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x63000000f401 at pc
0x0000004e744e bp 0x7ffc3c277010 sp 0x7ffc3c277008
READ of size 1 at 0x63000000f401 thread T0
#0 0x4e744d in void skip_group<__gnu_cxx::__normal_iterator<char*, std::__cxx11::basic_string<char,
std::char_traits, std::allocator > > >(__gnu_cxx::__normal_iterator<char*, std::__cxx11::basic_string<char,
std::char_traits, std::allocator > >&) /home/hjsz/rtf2html/./rtf_tools.h:27:15
#1 0x4db43c in main /home/hjsz/rtf2html/rtf2html.cpp:158:16
#2 0x7f7e99536082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
#3 0x41da0d in _start (/home/hjsz/rtf2html/rtf2html+0x41da0d)
0x63000000f401 is located 0 bytes to the right of 61441-byte region [0x630000000400,0x63000000f401)
allocated by thread T0 here:
#0 0x4c58bd in operator new(unsigned long) (/home/hjsz/rtf2html/rtf2html+0x4c58bd)
#1 0x7f7e999e635d in std::__cxx11::basic_string<char, std::char_traits, std::allocator >::_M_mutate(unsigned
long, unsigned long, char const*, unsigned long) (/lib/x86_64-linux-gnu/libstdc++.so.6+0x14335d)
SUMMARY: AddressSanitizer: heap-buffer-overflow /home/hjsz/rtf2html/./rtf_tools.h:27:15 in void
skip_group<__gnu_cxx::__normal_iterator<char*, std::__cxx11::basic_string<char, std::char_traits, std::allocator
> > >(__gnu_cxx::__normal_iterator<char*, std::__cxx11::basic_string<char, std::char_traits, std::allocator > >&)
Shadow bytes around the buggy address:
0x0c607fff9e30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c607fff9e40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c607fff9e50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c607fff9e60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c607fff9e70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c607fff9e80:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fff9e90: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fff9ea0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fff9eb0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fff9ec0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c607fff9ed0: 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
==3467450==ABORTING
```

Crash2 : SEGV on unknown address

```
=================================================================
AddressSanitizer:DEADLYSIGNAL
==3472093==ERROR: AddressSanitizer: SEGV on unknown address (pc 0x0000004d2be7 bp 0x7ffcfb04e1d0 sp 0x7ffcfb04d080 T0)
==3472093==The signal is caused by a READ memory access.
==3472093==Hint: this fault was caused by a dereference of a high value address (see register values below).
Dissassemble the provided pc to learn which register was used.
#0 0x4d2be7 in formatting_options::operator=(formatting_options const&) /home/hjsz/rtf2html/./fmt_opts.h:96:19
#1 0x4db0f9 in main /home/hjsz/rtf2html/rtf2html.cpp:572:21
#2 0x7f2556f85082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
#3 0x41da0d in _start (/home/hjsz/rtf2html/rtf2html+0x41da0d)

AddressSanitizer can not provide additional info.
SUMMARY: AddressSanitizer: SEGV /home/hjsz/rtf2html/./fmt_opts.h:96:19 in formatting_options::operator=(formatting_options const&)
==3472093==ABORTING
```

POC

POC.zip

Report of Information Security Laboratory of Ocean University of China @OUC_ISLOUC @OUC_Blue_Whale

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant