huntr

Buffer Over-read in function utf_ptr2char in vim/vim

0

✓ Valid Reported on May 21st 2022

Description

Buffer Over-read in function utf_ptr2char at mbyte.c:1794

vim version

```
git log
commit 31d9948e3a2529c2f619d56bdb48291dc261233d (HEAD -> master, tag: v8.2.
```

POC

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_
=================================================================
==3756371==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x62100
READ of size 1 at 0x621000013d00 thread T0
    #0 0xa464c8 in utf_ptr2char /home/fuzz/fuzz/vim/vim/src/mbyte.c:1794:9
    #1 0xaac9f3 in gchar_pos /home/fuzz/fuzz/vim/vim/src/misc1.c:523:9
    #2 0x10a9485 in findsent /home/fuzz/fuzz/vim/vim/src/textobject.c:50:6
    #3 0xa1b89e in getmark_buf_fnum /home/fuzz/fuzz/vim/vim/src/mark.c:354:
    #4 0xa1ae69 in getmark_buf /home/fuzz/fuzz/vim/vim/src/mark.c:287:12
    #5 0xda6891 in nfa_regmatch /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:
    #6 0xd96fd0 in nfa_regtry /home/fuzz/fuzz/vim/vim/src/./regexp_nfa.c:71
    #7 0xd94cb7 in nfa_regexec_both /home/fuzz/fuzz/vim/vim/src/./regexp_nf
    #8 0xcf6ed1 in nfa_regexec_multi /home/fuzz/fuzz/vim/vim/src/./regexp_r
    #9 0xcf3e72 in vim_regexec_multi /home/fuzz/fuzz/vim/vim/src/regexp.c:2
    #10 0x7af73f in ex_substitute /home/fuzz/fuzz/vim/vim/s
    #11 0x7dc8e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_
    #12 0x7c96a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
```

Chat with us

```
    #12 0x7c96a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #13 0xe5884c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:
    #14 0xe552a6 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:180
    #15 0xe54bdc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #16 0xe542be in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:120
    #17 0x7dc8e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #18 0x7c96a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:1
    #19 0x7ce2f1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #20 0x1424832 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #21 0x14209cb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #22 0x14160c5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #23 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #24 0x41ea6d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41ea6d)

0x621000013d00 is located 0 bytes to the right of 4096-byte region [0x62100
allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz-vim/vim/src/vim+0x499ccd)
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x142e2e5 in mf_alloc_bhdr /home/fuzz/fuzz/vim/vim/src/memfile.c:884
    #4 0x142d0f7 in mf_new /home/fuzz/fuzz/vim/vim/src/memfile.c:375:26
    #5 0xa620b8 in ml_new_data /home/fuzz/fuzz/vim/vim/src/memline.c:4080:1
    #6 0xa60a61 in ml_open /home/fuzz/fuzz/vim/vim/src/memline.c:394:15
    #7 0x50119a in open_buffer /home/fuzz/fuzz/vim/vim/src/buffer.c:186:9
    #8 0x142207c in create_windows /home/fuzz/fuzz/vim/vim/src/main.c:2875
    #9 0x142034a in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:711:5
    #10 0x14160c5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #11 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/vim/src
Shadow bytes around the buggy address:
  0x0c427fffa750: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa770: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa780: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c427fffa790: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c427fffa7a0:[fa]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c427fffa7f0: 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
==3756371==ABORTING
```

poc_h10_n_s.dat

Impact

This vulnerabilities are capable of crashing software, Modify Memory, and possible remote execution

References

- NVD Analysts give Base Score: 7.8 HIGH to similar issue
- NVD Analysts give Base Score: 7.8 HIGH to similar issue

CVE
CVE-2022-1927
(Published)

(Published)

Vulnerability Type
CWE-126: Buffer Over-read

Severity
High (7.8)

Registry
Other

Affected Version
*

Visibility
Public

Status
Fixed

Found by

TDHX ICS Security
@jieyongma
pro

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,603 times.

We are processing your report and will contact the **vim** team within 24 hours. 6 months ago

We have contacted a member of the **vim** team and are waiting to hear back 6 months ago

Bram Moolenaar 6 months ago Maintainer

I cannot reproduce it. I checked the code from the stack trace, and I don't see how this can happen. The message used is translated, do you have the locale set in the environment?

Chat with us

TDHX 6 months ago Researcher

TDHX Researcher

The env commond output:

```
SHELL=/bin/bash
SUDO_GID=1000
LC_ADDRESS=zh_CN.UTF-8
LC_NAME=zh_CN.UTF-8
SUDO_COMMAND=/usr/bin/su
LC_MONETARY=zh_CN.UTF-8
SUDO_USER=fuzz
PWD=/home/fuzz
LOGNAME=root
HOME=/root
LANG=en_US.UTF-8
LC_PAPER=zh_CN.UTF-8
LS_COLORS=rs=0:di=01;34:ln=01;36:mh=00:pi=40;33:so=01;35:do=01;35:bd=40;33;01:cd
LESSCLOSE=/usr/bin/lesspipe %s %s
TERM=xterm
LC_IDENTIFICATION=zh_CN.UTF-8
LESSOPEN=| /usr/bin/lesspipe %s
USER=root
DISPLAY=localhost:10.0
SHLVL=1
LC_TELEPHONE=zh_CN.UTF-8
LC_MEASUREMENT=zh_CN.UTF-8
LC_TIME=zh_CN.UTF-8
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/us
SUDO_UID=1000
MAIL=/var/mail/root
LC_NUMERIC=zh_CN.UTF-8
_=/usr/bin/env
```

Bram Moolenaar 6 months ago Maintainer

Can you still reproduce it when setting the whole environment to English?
There is not much I can do without knowing how to reproduce it.

TDHX 6 months ago

Hi

' '',

I tried to set the whole environment to English like this:

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim/src# export LC_ALL=en_US.UTF-8
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim/src# export LANGUAGE=en_US.UTF-8
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim/src# locale
LANG=en_US.UTF-8
LANGUAGE=en_US.UTF-8
LC_CTYPE="en_US.UTF-8"
LC_NUMERIC="en_US.UTF-8"
LC_TIME="en_US.UTF-8"
LC_COLLATE="en_US.UTF-8"
LC_MONETARY="en_US.UTF-8"
LC_MESSAGES="en_US.UTF-8"
LC_PAPER="en_US.UTF-8"
LC_NAME="en_US.UTF-8"
LC_ADDRESS="en_US.UTF-8"
LC_TELEPHONE="en_US.UTF-8"
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=en_US.UTF-8
```

Then run vim like this:

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim/src# ./vim -u NONE -i NONE -n -m -X -Z -e -s -
=================================================================
==52841==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000e81 at pc
READ of size 689 at 0x619000000e81 thread T0
    #0 0x430bd5 in strlen (/home/fuzz/fuzz/vim/vim/src/vim+0x430bd5)
    #1 0x1436730 in msg_outtrans_attr /home/fuzz/fuzz/vim/vim/src/message.c:1551:44
    #2 0x143418a in msg_attr_keep /home/fuzz/fuzz/vim/vim/src/message.c:176:5
    #3 0x14348bd in msg_attr /home/fuzz/fuzz/vim/vim/src/message.c:123:12
    #4 0x143c9a9 in msg_trunc_attr /home/fuzz/fuzz/vim/vim/src/message.c:933:9
    #5 0x9cb1c4 in process_next_cpt_value /home/fuzz/fuzz/vim/vim/src/insexpand.c:3277
    #6 0x9c88b9 in ins_compl_get_exp /home/fuzz/fuzz/vim/vim/src/insexpand.c:3749:19
    #7 0x9c74a8 in find_next_completion_match /home/fuzz/fuzz/vim/vim/src/insexpand.c:
    #8 0x9bfed4 in ins_compl_next /home/fuzz/fuzz/vim/vim/src/insexpand.c:4099:9
    #9 0x9c094c in ins_complete /home/fuzz/fuzz/vim/vim/src/insexpand.c:4949:9
    #10 0x673009 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1283:10
    #11 0xb6a57c in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028:9
    #12 0xb6c294 in n_opencmd /home/fuzz/fuzz/vim/vim/src/normal.c:62
    #13 0xb52a46 in nv_open /home/fuzz/fuzz/vim/vim/src/normal.c:74
    #14 0xb1fed1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:9
    #15 0x813d5e in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:6
    #16 0x813588 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8725:5
    #17 0x813139 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #18 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #19 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #20 0xe57a2c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1674:5
    #21 0xe54486 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:12
    #22 0xe53dbc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174:14
    #23 0xe5349e in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200:2
    #24 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #25 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #26 0x7cdc51 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:586:12
    #27 0x1423782 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #28 0x141f91b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #29 0x1415015 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #30 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/
    #31 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x619000000e81 is located 0 bytes to the right of 1025-byte region [0x619000000a80,0x6
allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz/vim/vim/src/vim+0x499ccd)
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x141507a in common_init /home/fuzz/fuzz/vim/vim/src/main.c:914:19
    #4 0x1414564 in main /home/fuzz/fuzz/vim/vim/src/main.c:185:5
    #5 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/l

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz/vim/vim/src/vim+0x43
Shadow bytes around the buggy address:
  0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
  ==52841==ABORTING
```

I also tried on another newly installed ubuntu 20.04. The issue is still reproduced.
Then, I pull the newest code to 8.2.5013

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# git log
commit 78d52883e10d71f23ab72a3d8b9733b00da8c9ad (HEAD -> master, tag: v8.2.5013, origi
```

Rebuild vim like this:

```
make distclean
export CFLAGS="-g -O0 -lpthread -fsanitize=address"
export CXXFLAGS="-g -O0 -lpthread -fsanitize=address"
export LDFLAGS="-fsanitize=address"
./configure --with-features=huge --enable-gui=none
make -j
```

Here is the output:

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# ./src/vim -u NONE -i NONE -n -m -X -Z -e -s -
=================================================================
==65307==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6
READ of size 689 at 0x619000000e81 thread T0
    #0 0x7ffff75eaa7c in __interceptor_strlen ../../../../src/libsani
    #1 0x555555e07295 in msg_outtrans_attr /home/fuzz/fuzz/vim/vim/src/message.c:1551
    #2 0x555555e00aee in msg_attr_keep /home/fuzz/fuzz/vim/vim/src/message.c:176
    #3 0x555555e008c3 in msg_attr /home/fuzz/fuzz/vim/vim/src/message.c:123
    #4 0x555555e03fe4 in msg_trunc_attr /home/fuzz/fuzz/vim/vim/src/message.c:933
    #5 0x555555900015 in process_next_cpt_value /home/fuzz/fuzz/vim/vim/src/insexpand.
    #6 0x555555902cb0 in ins_compl_get_exp /home/fuzz/fuzz/vim/vim/src/insexpand.c:374
    #7 0x5555559039b1 in find_next_completion_match /home/fuzz/fuzz/vim/vim/src/insexp
    #8 0x555555903d7e in ins_compl_next /home/fuzz/fuzz/vim/vim/src/insexpand.c:4099
    #9 0x555555906f04 in ins_complete /home/fuzz/fuzz/vim/vim/src/insexpand.c:4949
    #10 0x5555557607cd in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1283
    #11 0x5555559d5564 in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028
    #12 0x5555559d0174 in n_opencmd /home/fuzz/fuzz/vim/vim/src/normal.c:6275
    #13 0x5555559d7afb in nv_open /home/fuzz/fuzz/vim/vim/src/normal.c:7409
    #14 0x5555559adae5 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930
    #15 0x555555831f91 in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762
    #16 0x555555831d50 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8725
    #17 0x5555558315f4 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643
    #18 0x55555580e0b2 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #19 0x5555558052cf in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992
    #20 0x555555b2485f in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1674
    #21 0x555555b259ae in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801
    #22 0x555555b224d1 in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174
    #23 0x555555b22546 in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200
    #24 0x55555580e0b2 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567
    #25 0x5555558052cf in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992
    #26 0x555555803659 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:586
    #27 0x555555df9969 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106
    #28 0x555555df2bc0 in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780
    #29 0x555555df2473 in main /home/fuzz/fuzz/vim/vim/src/main.c:432
    #30 0x7ffff7205082 in __libc_start_main ../csu/libc-start.c:308
    #31 0x55555568ce4d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x138e4d)

0x619000000e81 is located 0 bytes to the right of 1025-byte region [0x619000000a80,0x6
allocated by thread T0 here:
    #0 0x7ffff7690808 in __interceptor_malloc ../../../../src/libsanitizer/asan/asan_m
    #1 0x55555568d292 in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246
    #2 0x55555568d07b in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151
    #3 0x555555df2de8 in common_init /home/fuzz/fuzz/vim/vim/src/main.c:914
    #4 0x555555df2179 in main /home/fuzz/fuzz/vim/vim/src/main.c:185
    #5 0x7ffff7205082 in __libc_start_main ../csu/libc-start.c:308

SUMMARY: AddressSanitizer: heap-buffer-overflow ../../../../src/libsanitizer/sanitizer
Shadow bytes around the buggy address:
  0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==65307==ABORTING
```

Here is the environment

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# locale
LANG=en_US.UTF-8
LANGUAGE=en_US.UTF-8
LC_CTYPE="en_US.UTF-8"
LC_NUMERIC="en_US.UTF-8"
LC_TIME="en_US.UTF-8"
LC_COLLATE="en_US.UTF-8"
LC_MONETARY="en_US.UTF-8"
LC_MESSAGES="en_US.UTF-8"
LC_PAPER="en_US.UTF-8"
LC_NAME="en_US.UTF-8"
LC_ADDRESS="en_US.UTF-8"
LC_TELEPHONE="en_US.UTF-8"
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=en_US.UTF-8
```

I noticed if I run vim which I built without any options, there is a E1187 output:

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# ./src/vim
E1187: Failed to source defaults.vim
Press ENTER or type command to continue
```

But if I run vim which is installed in ubuntu, there is no error hint.

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# vim
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim#
```

Here is the output of 'vim --version' which I built.

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# src/vim --version
VIM - Vi IMproved 8.2 (2019 Dec 12, compiled May 25 2022 00:16:50)
Included patches: 1-5013
Compiled by fuzz@fuzz-vm187
Huge version without GUI.  Features included (+) or not (-):
+acl               +file_in_path      +mouse_urxvt       -tag_any_white
+arabic            +find_in_path      +mouse_xterm       -tcl
+autocmd           +float             +multi_byte        +termguicolors
+autochdir         +folding           +multi_lang        +terminal
-autoservername    -footer            -mzscheme          +terminfo
-balloon_eval      +fork()            +netbeans_intg     +termresponse
+balloon_eval_term +gettext           +num64             +textobjects
-browse            -hangul_input      +packages          +textprop
++builtin_terms    +iconv             +path_extra        +timers
+byte_offset       +insert_expand     -perl              +title
+channel           +ipv6              +persistent_undo   -toolbar
+cindent           +job               +popupwin          +user_commands
-clientserver      +jumplist          +postscript        +vartabs
-clipboard         +keymap            +printer           +vertsplit
+cmdline_compl     +lambda            +profile           +vim9script
+cmdline_hist      +langmap           -python            +viminfo
+cmdline_info      +libcall           -python3           +virtualedit
+comments          +linebreak         +quickfix          +visual
+conceal           +lispindent        +reltime           +visualextra
+cryptv            +listcmds          +rightleft         +vreplace
```

```
+cscope            +localmap          -ruby              +wildignore
+cursorbind        -lua               +scrollbind        +wildmenu
+cursorshape       +menu              +signs             +windows
+dialog_con        +mksession         +smartindent       +writebackup
+diff              +modify_fname      -sodium            -X11
+digraphs          +mouse             -sound             -xfontset
-dnd               -mouseshape        +spell             -xim
-ebcdic            +mouse_dec         +startuptime       -xpm
+emacs_tags        -mouse_gpm         +statusline        -xsmp
+eval              -mouse_jsbterm     -sun_workshop      -xterm_clipboard
+ex_extra          +mouse_netterm     +syntax            -xterm_save
+extra_search      +mouse_sgr         +tag_binary
-farsi             -mouse_sysmouse    -tag_old_static
   system vimrc file: "$VIM/vimrc"
     user vimrc file: "$HOME/.vimrc"
 2nd user vimrc file: "~/.vim/vimrc"
      user exrc file: "$HOME/.exrc"
       defaults file: "$VIMRUNTIME/defaults.vim"
  fall-back for $VIM: "/usr/local/share/vim"
Compilation: gcc -c -I. -Iproto -DHAVE_CONFIG_H -g -O0 -lpthread -fsanitize=address -D
Linking: gcc -fsanitize=address -L/usr/local/lib -Wl,--as-needed -o vim -lm -ltinfo -l
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim#
```

Here is the output of 'vim --version' which is installed from ubuntu

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim# vim --version
VIM - Vi IMproved 8.1 (2018 May 18, compiled Feb 01 2022 09:16:32)
Included patches: 1-2269, 3612, 3625, 3669, 3741
Modified by team+vim@tracker.debian.org
Compiled by team+vim@tracker.debian.org
Huge version without GUI.  Features included (+) or not (-):
+acl               -farsi             -mouse_sysmouse    -tag_any_white
+arabic            +file_in_path      +mouse_urxvt       -tcl
+autocmd           +find_in_path      +mouse_xterm       +termguicolors
+autochdir         +float             +multi_byte        +terminal
-autoservername    +folding           +multi_lang        +terminfo
-balloon_eval      -footer            -mzscheme          +termresponse
+balloon_eval_term +fork()            +netbeans_intg     +textobjects
-browse            +gettext           +num64             +textprop
++builtin_terms    -hangul_input      +packages          +timers
+byte_offset       +iconv             +path_extra        +title
+channel           +insert_expand     -perl              -toolbar
+cindent           +job               +persistent_undo   +user_comman
-clientserver      +jumplist          +postscript        +vartabs
```

```
-clipboard         +keymap            +printer           +vertsplit
+cmdline_compl     +lambda            +profile           +virtualedit
+cmdline_hist      +langmap           -python            +visual
+cmdline_info      +libcall           +python3           +visualextra
+comments          +linebreak         +quickfix          +viminfo
+conceal           +lispindent        +reltime           +vreplace
+cryptv            +listcmds          +rightleft         +wildignore
+cscope            +localmap          -ruby              +wildmenu
+cursorbind        -lua               +scrollbind        +windows
+cursorshape       +menu              +signs             +writebackup
+dialog_con        +mksession         +smartindent       -X11
+diff              +modify_fname      +sound             -xfontset
+digraphs          +mouse             +spell             -xim
-dnd               -mouseshape        +startuptime       -xpm
-ebcdic            +mouse_dec         +statusline        -xsmp
+emacs_tags        +mouse_gpm         -sun_workshop      -xterm_clipboard
+eval              -mouse_jsbterm     +syntax            -xterm_save
+ex_extra          +mouse_netterm     +tag_binary
+extra_search      +mouse_sgr         -tag_old_static
   system vimrc file: "$VIM/vimrc"
     user vimrc file: "$HOME/.vimrc"
 2nd user vimrc file: "~/.vim/vimrc"
      user exrc file: "$HOME/.exrc"
       defaults file: "$VIMRUNTIME/defaults.vim"
  fall-back for $VIM: "/usr/share/vim"
Compilation: gcc -c -I. -Iproto -DHAVE_CONFIG_H   -Wdate-time  -g -O2 -fdebug-prefix-m
Linking: gcc   -Wl,-Bsymbolic-functions -Wl,-z,relro -Wl,-z,now -Wl,--as-needed -o vim
```

Hope all this information could help.

TDHX 6 months ago Researcher

Here is a new poc file to trigger the same issue:
poc_h15_s.dat

```
root@fuzz-vm187:/home/fuzz/fuzz/vim/vim/src# ./vim -u NONE -i NONE -n -m -X -Z -e -s -
=================================================================
==72312==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000e81 at pc
READ of size 689 at 0x619000000e81 thread T0
    #0 0x430bd5 in strlen (/home/fuzz/fuzz/vim/vim/src/vim+0x430bd5)
    #1 0x1436d10 in msg_outtrans_attr /home/fuzz/fuzz/vim/vim/src/me
    #2 0x143476a in msg_attr_keep /home/fuzz/fuzz/vim/vim/src/message.c:176:5
```

Chat with us

```
    #3 0x1434e9d in msg_attr /home/fuzz/fuzz/vim/vim/src/message.c:123:12
    #4 0x143cf89 in msg_trunc_attr /home/fuzz/fuzz/vim/vim/src/message.c:933:9
    #5 0x9cb2d4 in process_next_cpt_value /home/fuzz/fuzz/vim/vim/src/insexpand.c:3277
    #6 0x9c89c9 in ins_compl_get_exp /home/fuzz/fuzz/vim/vim/src/insexpand.c:3749:19

    #7 0x9c75b8 in find_next_completion_match /home/fuzz/fuzz/vim/vim/src/insexpand.c:
    #8 0x9bffe4 in ins_compl_next /home/fuzz/fuzz/vim/vim/src/insexpand.c:4099:9
    #9 0x9c0a5c in ins_complete /home/fuzz/fuzz/vim/vim/src/insexpand.c:4949:9
    #10 0x6730a9 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1283:10
    #11 0xb6a68c in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028:9
    #12 0xb4d855 in nv_edit /home/fuzz/fuzz/vim/vim/src/normal.c:6998:2
    #13 0xb1ffe1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
    #14 0x813dfe in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:6
    #15 0x813628 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8725:5
    #16 0x8131d9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #17 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #18 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #19 0xe57b3c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1674:5
    #20 0xe54596 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:12
    #21 0xe53ecc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174:14
    #22 0xe535ae in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200:2
    #23 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #24 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #25 0x7cdcf1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:586:12
    #26 0x1423d62 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #27 0x141fefb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #28 0x14155f5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #29 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/
    #30 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x619000000e81 is located 0 bytes to the right of 1025-byte region [0x619000000a80,0x6
allocated by thread T0 here:
    #0 0x499ccd in malloc (/home/fuzz/fuzz/vim/vim/src/vim+0x499ccd)
    #1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
    #2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
    #3 0x141565a in common_init /home/fuzz/fuzz/vim/vim/src/main.c:914:19
    #4 0x1414b44 in main /home/fuzz/fuzz/vim/vim/src/main.c:185:5
    #5 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/l

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz/vim/vim/src/vim+0x43
Shadow bytes around the buggy address:
  0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c327fff81f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c327fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

```
    0x0c327fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
    0x0c327fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  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
  ==72312==ABORTING
```

TDHX 6 months ago Researcher

Here is another poc file to trigger the same issue:
poc_h13_s.dat

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S /mnt/share/max/fuzz/poc/vim/poc_h13_s.dat -c :qa!
=================================================================
==2268484==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x619000000e81 at pc
0x000000430bd6 bp 0x7fffffff70b0 sp 0x7fffffff6870
READ of size 689 at 0x619000000e81 thread T0
#0 0x430bd5 in strlen (/home/fuzz/fuzz-vim/vim/src/vim+0x430bd5)
#1 0x1436d10 in msg_outtrans_attr /home/fuzz/fuzz/vim/vim/src/message.c:1551:44
#2 0x143476a in msg_attr_keep /home/fuzz/fuzz/vim/vim/src/message.c:176:5
#3 0x1434e9d in msg_attr /home/fuzz/fuzz/vim/vim/src/message.c:123:12
#4 0x143cf89 in msg_trunc_attr /home/fuzz/fuzz/vim/vim/src/message.c:933:9
#5 0x9cb2d4 in process_next_cpt_value /home/fuzz/fuzz/vim/vim/src/insexpan
#6 0x9c89c9 in ins_compl_get_exp /home/fuzz/fuzz/vim/vim/src/insexpand.c:
#7 0x9c75b8 in find_next_completion_match /home/fuzz/fuzz/vim/vim/src/inse
#8 0x9bffe4 in ins_compl_next /home/fuzz/fuzz/vim/vim/src/insexpand.c:4099:9
```

```
#9 0x9c0a5c in ins_complete /home/fuzz/fuzz/vim/vim/src/insexpand.c:4949:9
#10 0x6730a9 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:1283:10
#11 0xb6a68c in invoke_edit /home/fuzz/fuzz/vim/vim/src/normal.c:7028:9
#12 0xb6c3a4 in n_opencmd /home/fuzz/fuzz/vim/vim/src/normal.c:6275:6
#13 0xb52b56 in nv_open /home/fuzz/fuzz/vim/vim/src/normal.c:7409:2
#14 0xb1ffe1 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:930:5
#15 0x813dfe in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:6
#16 0x813628 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8725:5
#17 0x8131d9 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
#18 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
#19 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
#20 0xe57b3c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1674:5
#21 0xe54596 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:12
#22 0xe53ecc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1174:14
#23 0xe535ae in ex_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1200:2
#24 0x7dc2e9 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
#25 0x7c90a5 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
#26 0x7cdcf1 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:586:12
#27 0x1423d62 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
#28 0x141fefb in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
#29 0x14155f5 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
#30 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16
#31 0x41ea6d in _start (/home/fuzz/fuzz-vim/vim/src/vim+0x41ea6d)

0x619000000e81 is located 0 bytes to the right of 1025-byte region
[0x619000000a80,0x619000000e81)
allocated by thread T0 here:
#0 0x499ccd in malloc (/home/fuzz/fuzz-vim/vim/src/vim+0x499ccd)
#1 0x4cb3aa in lalloc /home/fuzz/fuzz/vim/vim/src/alloc.c:246:11
#2 0x4cb28a in alloc /home/fuzz/fuzz/vim/vim/src/alloc.c:151:12
#3 0x141565a in common_init /home/fuzz/fuzz/vim/vim/src/main.c:914:19
#4 0x1414b44 in main /home/fuzz/fuzz/vim/vim/src/main.c:185:5
#5 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz/fuzz-vim/vim/src/vim+0x430bd5)
in strlen
Shadow bytes around the buggy address:
0x0c327fff8180: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff8190: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff81a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff81b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0x0c327fff81c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0c327fff81d0:[01]fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c327fff81f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c327fff8200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c327fff8210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x0c327fff8220: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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
==2268484==ABORTING
```

Bram Moolenaar 6 months ago Maintainer

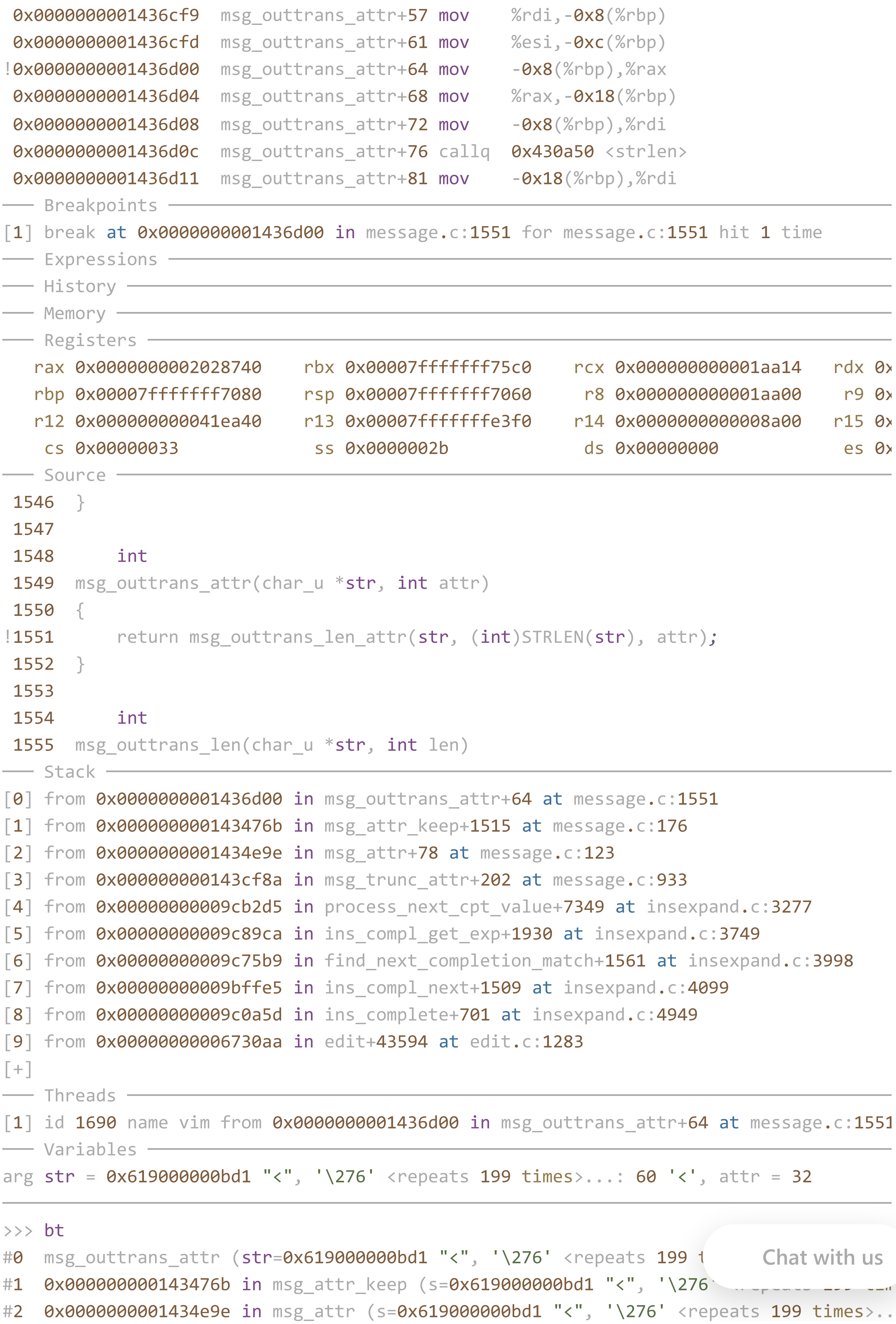
I cannot reproduce the problem. And as before, looking at the stack trace I cannot see any hint about what could be causing a problem like this.

TDHX 6 months ago Researcher

Could the gdb output help?

```
─── Output/messages ───────────────────────────────────────────────────────
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, msg_outtrans_attr (str=0x619000000bd1 "<", '\276' <repeats 199 times>...
1551        return msg_outtrans_len_attr(str, (int)STRLEN(str), attr);
─── Assembly ──────────────────────────────────────────────────────────────
 0x0000000001436cf0  msg_outtrans_attr+48 add    %r8b,%dl
 0x0000000001436cf3  msg_outtrans_attr+51 movslq %ecx,%rcx
 0x0000000001436cf6  msg_outtrans_attr+54 mov    %dl,(%rax,%rcx,1)
```



```
 0x0000000001436cf9  msg_outtrans_attr+57 mov    %rdi,-0x8(%rbp)
 0x0000000001436cfd  msg_outtrans_attr+61 mov    %esi,-0xc(%rbp)
!0x0000000001436d00  msg_outtrans_attr+64 mov    -0x8(%rbp),%rax
 0x0000000001436d04  msg_outtrans_attr+68 mov    %rax,-0x18(%rbp)
 0x0000000001436d08  msg_outtrans_attr+72 mov    -0x8(%rbp),%rdi
 0x0000000001436d0c  msg_outtrans_attr+76 callq  0x430a50 <strlen>
 0x0000000001436d11  msg_outtrans_attr+81 mov    -0x18(%rbp),%rdi
─── Breakpoints ────────────────────────────────────────────────────────────────────
[1] break at 0x0000000001436d00 in message.c:1551 for message.c:1551 hit 1 time
─── Expressions ────────────────────────────────────────────────────────────────────
─── History ────────────────────────────────────────────────────────────────────────
─── Memory ─────────────────────────────────────────────────────────────────────────
─── Registers ──────────────────────────────────────────────────────────────────────
   rax 0x0000000002028740     rbx 0x00007fffffff75c0     rcx 0x000000000001aa14     rdx 0x
   rbp 0x00007fffffff7080     rsp 0x00007fffffff7060      r8 0x000000000001aa00      r9 0x
   r12 0x000000000041ea40     r13 0x00007fffffffe3f0     r14 0x0000000000008a00     r15 0x
    cs 0x00000033              ss 0x0000002b              ds 0x00000000              es 0x
─── Source ─────────────────────────────────────────────────────────────────────────
 1546   }
 1547
 1548       int
 1549   msg_outtrans_attr(char_u *str, int attr)
 1550   {
!1551       return msg_outtrans_len_attr(str, (int)STRLEN(str), attr);
 1552   }
 1553
 1554       int
 1555   msg_outtrans_len(char_u *str, int len)
─── Stack ──────────────────────────────────────────────────────────────────────────
[0] from 0x0000000001436d00 in msg_outtrans_attr+64 at message.c:1551
[1] from 0x000000000143476b in msg_attr_keep+1515 at message.c:176
[2] from 0x0000000001434e9e in msg_attr+78 at message.c:123
[3] from 0x000000000143cf8a in msg_trunc_attr+202 at message.c:933
[4] from 0x00000000009cb2d5 in process_next_cpt_value+7349 at insexpand.c:3277
[5] from 0x00000000009c89ca in ins_compl_get_exp+1930 at insexpand.c:3749
[6] from 0x00000000009c75b9 in find_next_completion_match+1561 at insexpand.c:3998
[7] from 0x00000000009bffe5 in ins_compl_next+1509 at insexpand.c:4099
[8] from 0x00000000009c0a5d in ins_complete+701 at insexpand.c:4949
[9] from 0x00000000006730aa in edit+43594 at edit.c:1283
[+]
─── Threads ────────────────────────────────────────────────────────────────────────
[1] id 1690 name vim from 0x0000000001436d00 in msg_outtrans_attr+64 at message.c:1551
─── Variables ──────────────────────────────────────────────────────────────────────
arg str = 0x619000000bd1 "<", '\276' <repeats 199 times>...: 60 '<', attr = 32
────────────────────────────────────────────────────────────────────────────────────
>>> bt
#0  msg_outtrans_attr (str=0x619000000bd1 "<", '\276' <repeats 199 t
#1  0x000000000143476b in msg_attr_keep (s=0x619000000bd1 "<", '\276
#2  0x0000000001434e9e in msg_attr (s=0x619000000bd1 "<", '\276' <repeats 199 times>..
#3  0x000000000143cf8a in msg_trunc_attr (s=0x619000000a80 "Scanning tags.", force=1,
#4  0x00000000009cb2d5 in process_next_cpt_value (st=0x200d9a0 <ins_compl_get_exp.st>,
#5  0x00000000009c89ca in ins_compl_get_exp (ini=0x200d960 <compl_startpos>) at insexp
#6  0x00000000009c75b9 in find_next_completion_match (allow_get_expansion=1, todo=0, a
#7  0x00000000009bffe5 in ins_compl_next (allow_get_expansion=1, count=1, insert_match
#8  0x00000000009c0a5d in ins_complete (c=14, enable_pum=1) at insexpand.c:4949
#9  0x00000000006730aa in edit (cmdchar=111, startln=1, count=1) at edit.c:1283
#10 0x0000000000b6a68d in invoke_edit (cap=0x7fffffff8140, repl=0, cmd=111, startln=1)
#11 0x0000000000b6c3a5 in n_opencmd (cap=0x7fffffff8140) at normal.c:6275
#12 0x0000000000b52b57 in nv_open (cap=0x7fffffff8140) at normal.c:7409
#13 0x0000000000b1ffe2 in normal_cmd (oap=0x7fffffff8740, toplevel=1) at normal.c:930
#14 0x0000000000813dff in exec_normal (was_typed=0, use_vpeekc=0, may_use_terminal_loc
#15 0x0000000000813629 in exec_normal_cmd (cmd=0x611000000548 "0o\016", remap=0, siler
#16 0x00000000008131da in ex_normal (eap=0x7fffffff8cc0) at ex_docmd.c:8643
#17 0x00000000007dc2ea in do_one_cmd (cmdlinep=0x7fffffffa220, flags=7, cstack=0x7ffff
#18 0x00000000007c90a6 in do_cmdline (cmdline=0x6110000002c0 "se encoding=iso8859", fg
#19 0x0000000000e57b3d in do_source_ext (fname=0x603000000d93 "./poc_h10_s.dat", check
#20 0x0000000000e54597 in do_source (fname=0x603000000d93 "./poc_h10_s.dat", check_oth
#21 0x0000000000e53ecd in cmd_source (fname=0x603000000d93 "./poc_h10_s.dat", eap=0x7f
#22 0x0000000000e535af in ex_source (eap=0x7fffffffbc00) at scriptfile.c:1200
#23 0x00000000007dc2ea in do_one_cmd (cmdlinep=0x7fffffffd160, flags=11, cstack=0x7fff
#24 0x00000000007c90a6 in do_cmdline (cmdline=0x603000000a60 "so ./poc_h10_s.dat", fge
#25 0x00000000007cdcf2 in do_cmdline_cmd (cmd=0x603000000a60 "so ./poc_h10_s.dat") at
#26 0x0000000001423d63 in exe_commands (parmp=0x20210a0 <params>) at main.c:3106
#27 0x000000000141fefc in vim_main2 () at main.c:780
#28 0x00000000014155f6 in main (argc=15, argv=0x7fffffffe3f8) at main.c:432
>>>
```

We have sent a follow up to the **vim** team. We will try again in 7 days. 6 months ago

TDHX ICS Security modified the report 6 months ago

TDHX 6 months ago

Researcher

Found another Buffer Over-read at mbyte.c:1794. wish you could reproduce this one.
report is modified accordingly

Bram Moolenaar 6 months ago

OK, now I can reproduce it, and the POC is very simple. Problem is that the line number is zero.

Bram Moolenaar validated this vulnerability 6 months ago

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar marked this as fixed in 8.2 with commit 4d97a5 6 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Bram Moolenaar 6 months ago Maintainer

Fixed in patch 8.2.5037

Sign in to join this conversation