Out-of-bounds read in function gchar_cursor in vim/vim

0

Valid Reported on May 23rd 2022

Description

Out-of-bounds read in function gchar_cursor at misc1.c:532

vim version

```
git log
commit 68e64d2c1735f2a39afa8a0475ae29bedb116684 (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
==================================================================
==49778==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6210000
READ of size 1 at 0x621000013d07 thread T0
    #0 0xaac079 in gchar_cursor /home/fuzz/fuzz/vim/vim/src/misc1.c:532:17
    #1 0x66a034 in edit /home/fuzz/fuzz/vim/vim/src/edit.c:293:9
    #2 0xb21515 in normal_cmd /home/fuzz/fuzz/vim/vim/src/normal.c:1036:12
    #3 0x813d5e in exec_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8762:
    #4 0x813588 in exec_normal_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8
    #5 0x813139 in ex_normal /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:8643:6
    #6 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #7 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
    #8 0xe57a2c in do_source_ext /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1
    #9 0xe54486 in do_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:1801:
    #10 0xe53dbc in cmd_source /home/fuzz/fuzz/vim/vim/src/scriptfile.c:117
    #11 0xe5349e in ex_source /home/fuzz/fuzz/vim/vim/src/s
    #12 0x7dc249 in do_one_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:2567:2
    #13 0x7c9005 in do_cmdline /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:992:17
```

```
    #14 0x7cdc51 in do_cmdline_cmd /home/fuzz/fuzz/vim/vim/src/ex_docmd.c:5
    #15 0x1423782 in exe_commands /home/fuzz/fuzz/vim/vim/src/main.c:3106:2
    #16 0x141f91b in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:780:2
    #17 0x1415015 in main /home/fuzz/fuzz/vim/vim/src/main.c:432:12
    #18 0x7ffff7bec082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #19 0x41ea6d in _start (/home/fuzz/fuzz/vim/vim/src/vim+0x41ea6d)

0x621000013d07 is located 7 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 0x142d235 in mf_alloc_bhdr /home/fuzz/fuzz/vim/vim/src/memfile.c:884
    #4 0x142c047 in mf_new /home/fuzz/fuzz/vim/vim/src/memfile.c:375:26
    #5 0xa61528 in ml_new_data /home/fuzz/fuzz/vim/vim/src/memline.c:4082:1
    #6 0xa5fed1 in ml_open /home/fuzz/fuzz/vim/vim/src/memline.c:394:15
    #7 0x50117a in open_buffer /home/fuzz/fuzz/vim/vim/src/buffer.c:186:9
    #8 0x1420fcc in create_windows /home/fuzz/fuzz/vim/vim/src/main.c:2875:
    #9 0x141f29a in vim_main2 /home/fuzz/fuzz/vim/vim/src/main.c:711:5
    #10 0x1415015 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
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
==49778==ABORTING
```

poc_h11_s.dat

Impact

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

CVE
CVE-2022-1851
(Published)

Vulnerability Type
CWE-125: Out-of-bounds 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 1,237 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

Well, the POC is a bit complicated. I managed to simplify it a bit and pinpoint the actual problem: the cursor is left after the end of the line when formatting text. It's hard to make something simpler to reproduce the problem.

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 **78d528** 6 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

This vulnerability will not receive a CVE ✖

Bram Moolenaar 6 months ago Maintainer

Fixed in patch 8.2.5013

Sign in to join this conversation