huntr

Out-of-bounds Read in function get_lisp_indent in vim/vim

0

✓ Valid Reported on Jun 20th 2022

Description

Out-of-bounds Read in function get_lisp_indent at indent.c:2083

vim version

```
git log
commit e366ed4f2c6fa8cb663f1b9599b39d57ddbd8a2a (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_


=================================================================
==11737==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x621000
READ of size 1 at 0x621000013d00 thread T0
    #0 0x9a1d13 in get_lisp_indent /home/fuzz/fuzz/vim/afl/src/indent.c:20
    #1 0x99f321 in op_reindent /home/fuzz/fuzz/vim/afl/src/indent.c:1101:1
    #2 0xbb0d6d in do_pending_operator /home/fuzz/fuzz/vim/afl/src/ops.c:4
    #3 0xb1fd43 in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:961:2
    #4 0x814fee in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8809
    #5 0x814818 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #6 0x8143c9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex
    #7 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/e
    #8 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #9 0xe5928e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1
    #10 0xe55d26 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #11 0xe55663 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117

    #12 0xe54d6e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1206
    #13 0x7dd349 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #14 0x7ca205 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #15 0x7cee81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #16 0x1423142 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #17 0x141f2db in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #18 0x14147ed in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #19 0x7ffff7bed082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #20 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x621000013d00 is located 0 bytes to the right of 4096-byte region [0x62100
allocated by thread T0 here:
    #0 0x499cbd in malloc (/home/fuzz/fuzz/vim/afl/src/vim+0x499cbd)
    #1 0x4cb392 in lalloc /home/fuzz/fuzz/vim/afl/src/alloc.c:246:11
    #2 0x4cb27a in alloc /home/fuzz/fuzz/vim/afl/src/alloc.c:151:12
    #3 0x142ca45 in mf_alloc_bhdr /home/fuzz/fuzz/vim/afl/src/memfile.c:884
    #4 0x142b857 in mf_new /home/fuzz/fuzz/vim/afl/src/memfile.c:375:26
    #5 0xa61068 in ml_new_data /home/fuzz/fuzz/vim/afl/src/memline.c:4080:1
    #6 0xa5fa11 in ml_open /home/fuzz/fuzz/vim/afl/src/memline.c:394:15
    #7 0x501c9a in open_buffer /home/fuzz/fuzz/vim/afl/src/buffer.c:186:9
    #8 0x142098c in create_windows /home/fuzz/fuzz/vim/afl/src/main.c:2902:
    #9 0x141ec5a in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:711:5
    #10 0x14147ed in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #11 0x7ffff7bed082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/fuzz/fuzz/vim/afl/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
  0x0c427fffa7d0: 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
==11737==ABORTING
```

poc_obr2_s.dat

Impact

This vulnerability is capable of crashing software, modify memory, and possible remote execution.

CVE
CVE-2022-2183
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

Severity
High (7.8)

Chat with us

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 724 times.

We are processing your report and will contact the **vim** team within 24 hours. 5 months ago

We have contacted a member of the **vim** team and are waiting to hear back 5 months ago

Bram Moolenaar validated this vulnerability 5 months ago

I can reproduce the problem. I can use the POC to create a regression test. It can be simplified a bit more.

TDHX ICS Security has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Chat with us

Bram Moolenaar 5 months ago

Fixed with patch 8.2.5151

Bram Moolenaar marked this as fixed in 8.2 with commit 8eba2b 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation