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

0

Valid Reported on Jun 16th 2022

Description

Out-of-bounds Read in function suggest_trie_walk at spellsuggest.c:1437

vim version

```
git log
commit 83497f875881973df772cc4cc593766345df6c4a (HEAD -> master, tag: v8.2.
```

POC

```
root@fuzz-vm0-187:/home/fuzz/fuzz/vim/afl/src# ./vim -u NONE -i NONE -n -m
================================================================
==25892==ERROR: AddressSanitizer: stack-buffer-overflow on address 0x7ffcd4
READ of size 1 at 0x7ffcd478687f thread T0
    #0 0xf6de19 in suggest_trie_walk /home/fuzz/fuzz/vim/afl/src/spellsugge
    #1 0xf6a08d in suggest_try_change /home/fuzz/fuzz/vim/afl/src/spellsugg
    #2 0xf61979 in spell_suggest_intern /home/fuzz/fuzz/vim/afl/src/spellsu
    #3 0xf5ce9a in spell_find_suggest /home/fuzz/fuzz/vim/afl/src/spellsugg
    #4 0xf5879d in spell_suggest /home/fuzz/fuzz/vim/afl/src/spellsuggest.c
    #5 0xb63f84 in nv_zet /home/fuzz/fuzz/vim/afl/src/normal.c:3007:7
    #6 0xb1f59f in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:939:5
    #7 0x814eee in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8808:
    #8 0x814718 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/s
    #9 0x8142c9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex
    #10 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
```

```
    #11 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #12 0xe58b5e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #13 0xe555f6 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801

    #14 0xe54f33 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #15 0xe5463e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #16 0x7dd249 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #17 0x7ca105 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #18 0x7ced81 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #19 0x1422702 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #20 0x141e89b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #21 0x1413dad in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #22 0x7f3842261082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #23 0x41ea4d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea4d)

Address 0x7ffcd478687f is located in stack of thread T0 at offset 287 in fr
    #0 0xf69a5f in suggest_try_change /home/fuzz/fuzz/vim/afl/src/spellsugg

  This frame has 1 object(s):
    [32, 286) 'fword' (line 1185) <== Memory access at offset 287 overflows
HINT: this may be a false positive if your program uses some custom stack u
      (longjmp and C++ exceptions *are* supported)
SUMMARY: AddressSanitizer: stack-buffer-overflow /home/fuzz/fuzz/vim/afl/sr
Shadow bytes around the buggy address:
  0x10001a8e8cb0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8cc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8cd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8ce0: 00 00 00 00 00 00 00 00 00 00 00 00 f1 f1 f1 f1
  0x10001a8e8cf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x10001a8e8d00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00[06]
  0x10001a8e8d10: f3 f3 f3 f3 f3 f3 f3 f3 00 00 00 00 00 00 00 00
  0x10001a8e8d20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8d30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8d40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x10001a8e8d50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
  ==25892==ABORTING
```

poc_obr1_s.dat

Impact

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

CVE
CVE-2022-2126
(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 895 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 and found a fix.

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 5 months ago Maintainer

Fixed with Patch 8.2.5123

Bram Moolenaar marked this as fixed in **8.2** with commit **156d39** 5 months

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation