Out-of-bound read data in function suggest_trie_walk() abusing array byts in vim/vim

0

Valid Reported on Jun 27th 2022

Description

Out-of-bound read data in function `suggest_trie_walk()` abusing array `byts` in line spellsuggest.c:1925
Tested version: v8.2.5166

```
commit f65cc665fa751bad3ffe75f58ce1251d6695949f (HEAD -> master, tag: v8.2.
Author: Bram Moolenaar <Bram@vim.org>
Date:   Sun Jun 26 18:17:50 2022 +0100

    patch 8.2.5166: test for DiffUpdated fails

    Problem:    Test for DiffUpdated fails.
    Solution:   Also accept a count of two.
```

Proof of Concept

```
./vim -u NONE -i NONE -n -m -X -Z -e -s -S ./hbo_03.dat -c :qa!
```

```
==1678955==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60400
READ of size 1 at 0x604000001378 thread T0
    #0 0xd4d252 in suggest_trie_walk /home/h4niz/fuzz/vim/sync_dirs/vim/src
    #1 0xd31bc1 in suggest_try_change /home/h4niz/fuzz/vim/sync_dirs/vim/sr
    #2 0xd31bc1 in spell_suggest_intern /home/h4niz/fuzz/vi
    #3 0xd31bc1 in spell_find_suggest /home/h4niz/fuzz/vim/
    #4 0xd2e061 in spell_suggest /home/h4niz/fuzz/vim/sync_dirs/vim/src/spe
```

```
    #5 0x9fa872 in nv_zet /home/h4niz/fuzz/vim/sync_dirs/vim/src/normal.c:3
    #6 0x9c13b4 in normal_cmd /home/h4niz/fuzz/vim/sync_dirs/vim/src/normal
    #7 0x75d852 in exec_normal /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do

    #8 0x75c37a in exec_normal_cmd /home/h4niz/fuzz/vim/sync_dirs/vim/src/e
    #9 0x75c37a in ex_normal /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_docm
    #10 0x72f8f6 in do_one_cmd /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #11 0x72f8f6 in do_cmdline /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #12 0x71b247 in global_exe_one /home/h4niz/fuzz/vim/sync_dirs/vim/src/e
    #13 0x71b247 in global_exe /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_cm
    #14 0x71a89c in ex_global /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_cmd
    #15 0x72f8f6 in do_one_cmd /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #16 0x72f8f6 in do_cmdline /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #17 0xc79dbd in do_source_ext /home/h4niz/fuzz/vim/sync_dirs/vim/src/sc
    #18 0xc77683 in do_source /home/h4niz/fuzz/vim/sync_dirs/vim/src/script
    #19 0xc77683 in cmd_source /home/h4niz/fuzz/vim/sync_dirs/vim/src/scrip
    #20 0x72f8f6 in do_one_cmd /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #21 0x72f8f6 in do_cmdline /home/h4niz/fuzz/vim/sync_dirs/vim/src/ex_do
    #22 0x10c7796 in exe_commands /home/h4niz/fuzz/vim/sync_dirs/vim/src/ma
    #23 0x10c7796 in vim_main2 /home/h4niz/fuzz/vim/sync_dirs/vim/src/main.
    #24 0x10c37a0 in main /home/h4niz/fuzz/vim/sync_dirs/vim/src/main.c:432
    #25 0x7f7628d43082 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.
    #26 0x422ebd in _start (/home/h4niz/fuzz/vim/latest_vim/vim+0x422ebd)

0x604000001378 is located 0 bytes to the right of 40-byte region [0x6040000
allocated by thread T0 here:
    #0 0x49adbd in malloc (/home/h4niz/fuzz/vim/latest_vim/vim+0x49adbd)
    #1 0x4ca9ce in lalloc /home/h4niz/fuzz/vim/sync_dirs/vim/src/alloc.c:24

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/h4niz/fuzz/vim/sync_d
Shadow bytes around the buggy address:
  0x0c087fff8210: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fa
  0x0c087fff8220: fa fa fd fd fd fd fd fd fa fa fd fd fd fd fd fd
  0x0c087fff8230: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 05 fa
  0x0c087fff8240: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 05 fa
  0x0c087fff8250: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd fd
=>0x0c087fff8260: fa fa fd fd fd fd fd fd fa fa 00 00 00 00 00[fa]
  0x0c087fff8270: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8280: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c087fff8290: fa fa 00 00 00 00 00 00 fa fa fd fd fd fd fa fa
  0x0c087fff82a0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fa fa
```

```
  0x0c087fff82b0: fa fa fd fd fd fd fd fa fa fa fd fd fd fd fd 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
==1678955==ABORTING
```

Download POC: hbo_03.dat

Impact

This may result in corruption of sensitive information or a crash.

CVE
CVE-2022-2287
(Published)

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

Severity
High (8)

Registry
Other

Other

Affected Version
v8.2.5166

Visibility
Public

Status
Fixed

Found by

h4niz
@h4niz
amateur

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 744 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 5 months ago Maintainer

This POC is garbled and too long. Please reduce it to the absolute minimum to reproduce the problem.

h4niz 5 months ago Researcher

Here you are. hbo_03.dat

We have sent a follow up to the vim team. We will try again in 7 days. 5 mont

Bram Moolenaar 5 months ago Maintainer

I managed to reduce the POC further to see what part is actually causing trouble. Quite a puzzle, spell checking is a lot of code. I finally managed to pinpoint the problem and reproduce it in a test.

Bram Moolenaar validated this vulnerability 5 months ago

h4niz 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 9.0.0021

Bram Moolenaar marked this as fixed in **9.0** with commit **5e59ea** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation