huntr

Heap buffer overflow in vim_strncpy find_word in vim/vim

0

✓ Valid Reported on Apr 28th 2022

✍️ Description

When fuzzing vim commit `fc78a0369` (works with latest build and latest commit `202b4bd3a` per this time of this report) with clang 13 and ASan, I discovered a buffer overflow.

Proof of Concept

Here is the poc

```
https://drive.google.com/file/d/11yaq4umocSbwphl7o31r50it0IP2bYGE/view?usp=
```

How to build

```
LD=lld AS=llvm-as AR=llvm-ar RANLIB=llvm-ranlib CC=clang CXX=clang++ CFLAGS
make -j$(nproc)
```

Proof of Concept
Run crafted file with this command
`./vim -u NONE -X -Z -e -s -S poc_vim_strncpy_min -c :qa!`
ASan stack trace:

```
aldo@vps:~/vimbaru/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER_PATH=/usr/
=================================================================
==2676390==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60200
READ of size 1 at 0x602000007032 thread T0
SCARINESS: 12 (1-byte-read-heap-buffer-overflow)
    #0 0x485f0c  (/home/aldo/vimtes/src/vim+0x485f0c)
    #1 0xbd6554  (/home/aldo/vimtes/src/vim+0xbd6554)
    #1 0xbd6554  (/home/aldo/vimtes/src/vim+0xbd6554)
    #2 0xbb8e32  (/home/aldo/vimtes/src/vim+0xbb8e32)
    #3 0xbb3d63  (/home/aldo/vimtes/src/vim+0xbb3d63)
    #4 0xbb0303  (/home/aldo/vimtes/src/vim+0xbb0303)
    #5 0xbaccac  (/home/aldo/vimtes/src/vim+0xbaccac)
    #6 0x928db0  (/home/aldo/vimtes/src/vim+0x928db0)
    #7 0x8fa54d  (/home/aldo/vimtes/src/vim+0x8fa54d)
    #8 0x6fba0d  (/home/aldo/vimtes/src/vim+0x6fba0d)
    #9 0x6fb613  (/home/aldo/vimtes/src/vim+0x6fb613)
    #10 0x6fb373  (/home/aldo/vimtes/src/vim+0x6fb373)
    #11 0x6d6a92  (/home/aldo/vimtes/src/vim+0x6d6a92)
    #12 0x6ca7c2  (/home/aldo/vimtes/src/vim+0x6ca7c2)
    #13 0xafe285  (/home/aldo/vimtes/src/vim+0xafe285)
    #14 0xafbcd0  (/home/aldo/vimtes/src/vim+0xafbcd0)
    #15 0xafb809  (/home/aldo/vimtes/src/vim+0xafb809)
    #16 0xafb2ed  (/home/aldo/vimtes/src/vim+0xafb2ed)
    #17 0x6d6a92  (/home/aldo/vimtes/src/vim+0x6d6a92)
    #18 0x6ca7c2  (/home/aldo/vimtes/src/vim+0x6ca7c2)
    #19 0x6cda50  (/home/aldo/vimtes/src/vim+0x6cda50)
    #20 0xed9214  (/home/aldo/vimtes/src/vim+0xed9214)
    #21 0xed6f49  (/home/aldo/vimtes/src/vim+0xed6f49)
    #22 0xed0830  (/home/aldo/vimtes/src/vim+0xed0830)
    #23 0x7ffff78240b2  (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)
    #24 0x41edcd  (/home/aldo/vimtes/src/vim+0x41edcd)

0x602000007032 is located 0 bytes to the right of 2-byte region [0x60200000
allocated by thread T0 here:
    #0 0x499c8d  (/home/aldo/vimtes/src/vim+0x499c8d)
    #1 0x4cb0e0  (/home/aldo/vimtes/src/vim+0x4cb0e0)
    #2 0x4cb039  (/home/aldo/vimtes/src/vim+0x4cb039)
    #3 0xbd3c05  (/home/aldo/vimtes/src/vim+0xbd3c05)
    #4 0xbacb21  (/home/aldo/vimtes/src/vim+0xbacb21)
    #5 0x928db0  (/home/aldo/vimtes/src/vim+0x928db0)
    #6 0x8fa54d  (/home/aldo/vimtes/src/vim+0x8fa54d)
    #7 0x6fba0d  (/home/aldo/vimtes/src/vim+0x6fba0d)
    #8 0x6fb613  (/home/aldo/vimtes/src/vim+0x6fb613)
    #9 0x6fb373  (/home/aldo/vimtes/src/vim+0x6fb373)
    #10 0x6d6a92  (/home/aldo/vimtes/src/vim+0x6d6a92)
    #11 0x6ca7c2  (/home/aldo/vimtes/src/vim+0x6ca7c2)
    #12 0xafe285  (/home/aldo/vimtes/src/vim+0xafe285)
    #13 0xafbcd0  (/home/aldo/vimtes/src/vim+0xafbcd0)
    #14 0xafb809  (/home/aldo/vimtes/src/vim+0xafb809)
    #14 0xafb809  (/home/aldo/vimtes/src/vim+0xafb809)
    #15 0xafb2ed  (/home/aldo/vimtes/src/vim+0xafb2ed)
    #16 0x6d6a92  (/home/aldo/vimtes/src/vim+0x6d6a92)

    #17 0x6ca7c2  (/home/aldo/vimtes/src/vim+0x6ca7c2)
    #18 0x6cda50  (/home/aldo/vimtes/src/vim+0x6cda50)
    #19 0xed9214  (/home/aldo/vimtes/src/vim+0xed9214)
    #20 0xed6f49  (/home/aldo/vimtes/src/vim+0xed6f49)
    #21 0xed0830  (/home/aldo/vimtes/src/vim+0xed0830)
    #22 0x7ffff78240b2  (/lib/x86_64-linux-gnu/libc.so.6+0x240b2)

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/aldo/vimtes/src/vim+
Shadow bytes around the buggy address:
  0x0c047fff8db0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8dc0: fa fa fd fd fa fa fd fd fa fa fd fa fa fa 01 fa
  0x0c047fff8dd0: fa fa 00 00 fa fa 01 fa fa fa 02 fa fa fa 05 fa
  0x0c047fff8de0: fa fa fd fa fa fa 00 06 fa fa 00 07 fa fa fd fa
  0x0c047fff8df0: fa fa fd fd fa fa fd fa fa fa 01 fa fa fa 02 fa
=>0x0c047fff8e00: fa fa fd fa fa fa[02]fa fa fa 02 fa fa fa 05 fa
  0x0c047fff8e10: fa fa 04 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e50: 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

  ==2676390==ABORTING
  Aborted
```

valgrind output on vim no asan build

```
==2678356== Memcheck, a memory error detector
==2678356== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==2678356== Using Valgrind-3.15.0 and LibVEX; rerun with -h for copyright i
==2678356== Command: ./vim -u NONE -X -Z -e -s -S poc_vim_strncpy_min -c :c
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B8652: find_word (spell.c:476)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5B9D25: spell_move_to (spell.c:1363)
==2678356==    by 0x5CB5A4: spell_suggest (spellsuggest.c:515)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B867E: find_word (spell.c:490)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5B9D25: spell_move_to (spell.c:1363)
==2678356==    by 0x5CB5A4: spell_suggest (spellsuggest.c:515)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
```

```
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)

==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B86BA: find_word (spell.c:495)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5B9D25: spell_move_to (spell.c:1363)
==2678356==    by 0x5CB5A4: spell_suggest (spellsuggest.c:515)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B8925: find_word (spell.c:591)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5B9D25: spell_move_to (spell.c:1363)
==2678356==    by 0x5CB5A4: spell_suggest (spellsuggest.c:515)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
```

```
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)

==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B8652: find_word (spell.c:476)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5CBD27: spell_find_suggest (spellsuggest.c:796)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B867E: find_word (spell.c:490)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5CBD27: spell_find_suggest (spellsuggest.c:796)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
```

```
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==

==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B86BA: find_word (spell.c:495)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5CBD27: spell_find_suggest (spellsuggest.c:796)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5B8925: find_word (spell.c:591)
==2678356==    by 0x5B7C78: spell_check (spell.c:282)
==2678356==    by 0x5CBD27: spell_find_suggest (spellsuggest.c:796)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
```

```
==2678356==    at 0x5CF62E: suggest_trie_walk (spellsuggest.c:1433)
==2678356==    by 0x5CC469: suggest_try_change (spellsuggest.c:1212)
==2678356==    by 0x5CC469: spell_suggest_intern (spellsuggest.c:1008)

==2678356==    by 0x5CC469: spell_find_suggest (spellsuggest.c:883)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x6795DC: exe_commands (main.c:3108)
==2678356==    by 0x6795DC: vim_main2 (main.c:780)
==2678356==
==2678356== Conditional jump or move depends on uninitialised value(s)
==2678356==    at 0x5CE30F: suggest_trie_walk (spellsuggest.c:1892)
==2678356==    by 0x5CC469: suggest_try_change (spellsuggest.c:1212)
==2678356==    by 0x5CC469: spell_suggest_intern (spellsuggest.c:1008)
==2678356==    by 0x5CC469: spell_find_suggest (spellsuggest.c:883)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x6795DC: exe_commands (main.c:3108)
==2678356==    by 0x6795DC: vim_main2 (main.c:780)
  2678356
```

```
==2678356==
==2678356== Invalid read of size 1
==2678356==    at 0x483F269: strncpy (in /usr/lib/x86_64-linux-gnu/valgrind

==2678356==    by 0x5D357E: strncpy (string_fortified.h:106)
==2678356==    by 0x5D357E: vim_strncpy (strings.c:505)
==2678356==    by 0x5CDE42: check_suggestions (spellsuggest.c:3653)
==2678356==    by 0x5CC981: spell_suggest_intern (spellsuggest.c:1068)
==2678356==    by 0x5CC981: spell_find_suggest (spellsuggest.c:883)
==2678356==    by 0x5CB74B: spell_suggest (spellsuggest.c:554)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==  Address 0x5159872 is 0 bytes after a block of size 2 alloc'd
==2678356==    at 0x483B7F3: malloc (in /usr/lib/x86_64-linux-gnu/valgrind/
==2678356==    by 0x406567: lalloc (alloc.c:246)
==2678356==    by 0x5D2C1B: vim_strsave (strings.c:27)
==2678356==    by 0x5CB700: spell_suggest (spellsuggest.c:544)
==2678356==    by 0x500C8F: nv_zet (normal.c:2998)
==2678356==    by 0x4F8E73: normal_cmd (normal.c:930)
==2678356==    by 0x47E82C: exec_normal (ex_docmd.c:0)
==2678356==    by 0x47E6F1: exec_normal_cmd (ex_docmd.c:8720)
==2678356==    by 0x47E6F1: ex_normal (ex_docmd.c:8638)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==    by 0x5A5144: do_source_ext (scriptfile.c:1674)
==2678356==    by 0x5A47E6: do_source (scriptfile.c:1801)
==2678356==    by 0x5A47E6: cmd_source (scriptfile.c:1174)
==2678356==    by 0x477523: do_one_cmd (ex_docmd.c:2567)
==2678356==    by 0x477523: do_cmdline (ex_docmd.c:992)
==2678356==
==2678356==
==2678356== HEAP SUMMARY:
==2678356==     in use at exit: 140,324,083 bytes in 398 blocks
```

```
==2678356==   total heap usage: 1,309 allocs, 911 frees, 280,939,794 bytes
==2678356==
==2678356== LEAK SUMMARY:

==2678356==    definitely lost: 0 bytes in 0 blocks
==2678356==    indirectly lost: 0 bytes in 0 blocks
==2678356==      possibly lost: 0 bytes in 0 blocks
==2678356==    still reachable: 140,324,083 bytes in 398 blocks
==2678356==         suppressed: 0 bytes in 0 blocks
==2678356== Reachable blocks (those to which a pointer was found) are not s
==2678356== To see them, rerun with: --leak-check=full --show-leak-kinds=al
==2678356==
==2678356== Use --track-origins=yes to see where uninitialised values come
==2678356== For lists of detected and suppressed errors, rerun with: -s
==2678356== ERROR SUMMARY: 11 errors from 11 contexts (suppressed: 0 from 0
```

Impact

This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution

CVE
CVE-2022-1621
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.3)

Registry
Other

Affected Version
8.2.4843

Visibility
Public

Status
Fixed

Found by

Muhammad Aldo Firmansyah

@thecrott

legend

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,423 times.

We are processing your report and will contact the **vim** team within 24 hours. 7 months ago

Muhammad Aldo Firmansyah modified the report 7 months ago

We have contacted a member of the **vim** team and are waiting to hear back 7 months ago

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

Bram Moolenaar 7 months ago Maintainer

When I try to reproduce (using valgrind) Vim just appears to hang.

Muhammad Aldo Firmansyah modified the report 7 months ago

Muhammad 7 months ago Researcher

@brammool it's common thing after few more commits poc doesn't work anymore so I'm re-fuzz again and update the original post

Bram Moolenaar validated this vulnerability 7 months ago

I can reproduce it now. Adding illegal utf-8 bytes to the word tree causes prob'

Chat with us

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Bram Moolenaar 7 months ago Maintainer

Fixed in patch 8.2.4919

Bram Moolenaar marked this as fixed in 8.2 with commit 7c8246 7 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

xiaoge1001 6 months ago

@thecrott I'm very sorry. It's not convenient for me to visit the POC file download address and I can't download it. Can you provide the contents of the POC file here or upload the POC file to GitHub? Thank you very much.
I use vim-8.2. I analyze the code and think it is affected, but I need to reproduce the problem.

Sign in to join this conversation

FAQ

contact us

terms

privacy policy

Chat with us