huntr

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

0

✓ Valid Reported on Jun 29th 2022

Description

Out-of-bounds Read in function ins_bytes at change.c:968

vim version

```
git log
commit 9610f94510220c783328e1857af87a6ae7bc20b4 (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_obr4_s.dat -c :qa!
=================================================================
==2965871==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020
READ of size 1 at 0x6020000071b1 thread T0
    #0 0x430bc5 in strlen (/home/fuzz/fuzz/vim/afl/src/vim+0x430bc5)
    #1 0x54bfbd in ins_bytes /home/fuzz/fuzz/vim/afl/src/change.c:968:27
    #2 0x9bb1cc in ins_compl_stop /home/fuzz/fuzz/vim/afl/src/insexpand.c:2
    #3 0x9b9a65 in ins_compl_prep /home/fuzz/fuzz/vim/afl/src/insexpand.c:2
    #4 0x66f81a in edit /home/fuzz/fuzz/vim/afl/src/edit.c:688:6
    #5 0xb2233b in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:1045:12
    #6 0x8153de in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812:
    #7 0x814c08 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #8 0x8147b9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:6
    #9 0x7dd739 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #10 0x7ca5f5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/
    #11 0xe5b76e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #12 0xe58206 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #12 0xe58206 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:180
    #13 0xe57b43 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #14 0xe5724e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:120
    #15 0x7dd739 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #16 0x7ca5f5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #17 0x7cf271 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #18 0x1425db2 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:
    #19 0x1421f4b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #20 0x141745d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #21 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #22 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x6020000071b1 is located 0 bytes to the right of 1-byte region [0x60200000
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 0xf8faad in vim_strnsave /home/fuzz/fuzz/vim/afl/src/strings.c:44:9
    #4 0x9c2a61 in ins_compl_start /home/fuzz/fuzz/vim/afl/src/insexpand.c:
    #5 0x9c10bb in ins_complete /home/fuzz/fuzz/vim/afl/src/insexpand.c:49
    #6 0x674619 in edit /home/fuzz/fuzz/vim/afl/src/edit.c:1281:10
    #7 0xb2233b in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:1045:12
    #8 0x8153de in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812
    #9 0x814c08 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8
    #10 0x8147b9 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8693:
    #11 0x7dd739 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #12 0x7ca5f5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #13 0xe5b76e in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c
    #14 0xe58206 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:180
    #15 0xe57b43 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #16 0xe5724e in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:120
    #17 0x7dd739 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570
    #18 0x7ca5f5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:
    #19 0x7cf271 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #20 0x1425db2 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:
    #21 0x1421f4b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #22 0x141745d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #23 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow (/home/fuzz
Shadow bytes around the buggy address:
  0x0c047fff8de0: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c047fff8df0: fa fa fd fd fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c047fff8e00: fa fa fd fa fa fa fd fa fa fa fd fa fa fa 02 fa

  0x0c047fff8e10: fa fa 00 fa fa fa 02 fa fa fa fd fa fa fa fd fa
  0x0c047fff8e20: fa fa 04 fa fa fa 02 fa fa fa 02 fa fa fa fd fa
=>0x0c047fff8e30: fa fa 01 fa fa fa[01]fa fa fa 01 fa fa fa 03 fa
  0x0c047fff8e40: fa fa 06 fa fa fa fd fa fa fa fd fa fa fa 00 07
  0x0c047fff8e50: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c047fff8e80: 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
==2965871==ABORTING
```

poc_obr4_s.dat

Impact

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

CVE
CVE-2022-2286
(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 633 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 bac

Chat with us

TDHX ICS Security modified the report 5 months ago

TDHX 5 months ago Researcher

Noticed original issue(Out-of-bounds Read in function inc) was fixed with patch 9.0.0011.
So the report is updated to another Out-of-bounds Read issue(Out-of-bounds Read in function ins_bytes).

Bram Moolenaar validated this vulnerability 5 months ago

I can reproduce the problem. The POC can be simplified a bit more and then used as a regression test.

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 9.0.0020

Bram Moolenaar marked this as fixed in 9.0 with commit f12129 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us