huntr

Integer Overflow in function del_typebuf in vim/vim

0

✓ Valid Reported on Jun 29th 2022

Description

Integer Overflow in function del_typebuf at getchar.c:1204

vim version

```
git log
commit 75417d960bd17a5b701cfb625b8864dacaf0cc39 (HEAD -> master, tag: v9.0.
```

POC

```
./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_intof1_s.dat -c :q
=================================================================
==378387==ERROR: AddressSanitizer: negative-size-param: (size=-1)
    #0 0x49945c in __asan_memmove (/home/fuzz/fuzz/vim/afl/src/vim+0x49945c
    #1 0x918e70 in del_typebuf /home/fuzz/fuzz/vim/afl/src/getchar.c:1204:2
    #2 0x10332cb in put_string_in_typebuf /home/fuzz/fuzz/vim/afl/src/term.
    #3 0x103957d in check_termcode /home/fuzz/fuzz/vim/afl/src/term.c:5900:
    #4 0x930589 in handle_mapping /home/fuzz/fuzz/vim/afl/src/getchar.c:268
    #5 0x91fe8e in vgetorpeek /home/fuzz/fuzz/vim/afl/src/getchar.c:3143:29
    #6 0x91cf31 in vgetc /home/fuzz/fuzz/vim/afl/src/getchar.c:1720:10
    #7 0x925f1d in safe_vgetc /home/fuzz/fuzz/vim/afl/src/getchar.c:1951:9
    #8 0xb1cca5 in normal_cmd /home/fuzz/fuzz/vim/afl/src/normal.c:747:9
    #9 0x81539e in exec_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8812:
    #10 0x814bc8 in exec_normal_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:
    #11 0x814779 in ex_normal /home/fuzz/fuzz/vim/afl/src/e
    #12 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_
    #13 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
```

Chat with us

```
    #13 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #14 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:
    #15 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #16 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #17 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #18 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #19 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #20 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #21 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #22 0x142022b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #23 0x141573d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #24 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/
    #25 0x41ea5d in _start (/home/fuzz/fuzz/vim/afl/src/vim+0x41ea5d)

0x612000000678 is located 56 bytes inside of 265-byte region [0x61200000064
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 0x919da2 in alloc_typebuf /home/fuzz/fuzz/vim/afl/src/getchar.c:1340
    #4 0x91a5c9 in save_typeahead /home/fuzz/fuzz/vim/afl/src/getchar.c:141
    #5 0x812f94 in save_current_state /home/fuzz/fuzz/vim/afl/src/ex_docmd.
    #6 0x814406 in ex_normal /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:8677:9
    #7 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:2
    #8 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:17
    #9 0xe59ece in do_source_ext /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1
    #10 0xe56966 in do_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1801
    #11 0xe562a3 in cmd_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:117
    #12 0xe559ae in ex_source /home/fuzz/fuzz/vim/afl/src/scriptfile.c:1200
    #13 0x7dd6f9 in do_one_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:2570:
    #14 0x7ca5b5 in do_cmdline /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:992:1
    #15 0x7cf231 in do_cmdline_cmd /home/fuzz/fuzz/vim/afl/src/ex_docmd.c:5
    #16 0x1424092 in exe_commands /home/fuzz/fuzz/vim/afl/src/main.c:3133:2
    #17 0x142022b in vim_main2 /home/fuzz/fuzz/vim/afl/src/main.c:780:2
    #18 0x141573d in main /home/fuzz/fuzz/vim/afl/src/main.c:432:12
    #19 0x7ffff7bee082 in __libc_start_main /build/glibc-SzIz7B/glibc-2.31/

SUMMARY: AddressSanitizer: negative-size-param (/home/fuzz/fuzz/vim/afl/src
==378387==ABORTING
```

poc_intof1_s.dat

GDB

```
gdb --args ./afl/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S ./poc_intof1_

(gdb) b getchar.c:1204
Breakpoint 1 at 0x918d3c: file getchar.c, line 1204.
(gdb) r
Starting program: /home/fuzz/fuzz/vim/afl/src/vim -u NONE -i NONE -n -m -X
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Breakpoint 1, del_typebuf (len=4, offset=1) at getchar.c:1204
1204            mch_memmove(typebuf.tb_buf + typebuf.tb_off + offset,
(gdb) p typebuf.tb_len
$1 = -1
(gdb) p offset
$2 = 1
(gdb) l
1199                mch_memmove(typebuf.tb_noremap + MAXMAPLEN,
1200                                typebuf.tb_noremap + typebuf.tb_off, (size
1201                typebuf.tb_off = MAXMAPLEN;
1202            }
1203            // adjust typebuf.tb_buf (include the NUL at the end)
1204            mch_memmove(typebuf.tb_buf + typebuf.tb_off + offset,
1205                                                        typebuf.tb_buf
1206                                                (size_t)(typebuf.tb_len - of
1207            // adjust typebuf.tb_noremap[]
1208            mch_memmove(typebuf.tb_noremap + typebuf.tb_off + offset,
(gdb)
```

Impact

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

CVE

CVE-2022-2285
(Published)

Vulnerability Type
CWE-190: Integer Overflow or Wraparound

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 896 times.

We are processing your report and will contact the vim team within 24 hours. 5 months ago

TDHX ICS Security modified the report 5 months ago

We have contacted a member of the vim team and are waiting to hear back

Chat with us

Bram Moolenaar 5 months ago Maintainer

The POC gives me this error: Conditional jump or move depends on uninitialised value(s)

Bram Moolenaar validated this vulnerability 5 months ago

Let's assume that fixing the uninitialized access also fixes this problem.

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 9.0.0018

Bram Moolenaar marked this as fixed in 9.0 with commit 27efc6 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

company

about

team

Chat with us