Heap-based buffer overflow in function ins_bs in vim/vim

0

✓ Valid Reported on Jun 24th 2022

Description

Heap-based buffer overflow in function `ins_bs` at edit.c:4187

Version

```
commit 8eba2bd291b347e3008aa9e565652d51ad638cfa (HEAD, tag: v8.2.5151)
```

Proof of Concept

```
guest@elk:~/trung/vim2/src$ valgrind ./vim -u NONE -i NONE -n -m -X -Z -e -
==5251== Memcheck, a memory error detector
==5251== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==5251== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==5251== Command: ./vim -u NONE -i NONE -n -m -X -Z -e -s -S /home/guest/tr
==5251==
==5251== Invalid read of size 1
==5251==    at 0x13D952: ins_bs (edit.c:4187)
==5251==    by 0x181717: edit (edit.c:958)
==5251==    by 0x22F599: invoke_edit.isra.1 (normal.c:7035)
==5251==    by 0x2317D1: n_opencmd (normal.c:6279)
==5251==    by 0x2317D1: nv_open (normal.c:7416)
==5251==    by 0x2385B4: normal_cmd (normal.c:939)
==5251==    by 0x1B671C: exec_normal (ex_docmd.c:8807)
==5251==    by 0x1B697F: ex_normal (ex_docmd.c:8693)
==5251==    by 0x1BB29D: do_one_cmd (ex_docmd.c:2570)
==5251==    by 0x1BB29D: do_cmdline (ex_docmd.c:992)
==5251==    by 0x2ABF00: do_source_ext (scriptfile.c:1674)
==5251==    by 0x2ACEF3: do_source (scriptfile.c:1801)
==5251==    by 0x2ACEF3: cmd_source (scriptfile.c:1174)
```

```
==5251==    by 0x1BB29D: do_one_cmd (ex_docmd.c:2570)
==5251==    by 0x1BB29D: do_cmdline (ex_docmd.c:992)
==5251==    by 0x380A9F: exe_commands (main.c:3133)
==5251==    by 0x380A9F: vim_main2 (main.c:780)
==5251==  Address 0x61d994f is 1 bytes before a block of size 6 alloc'd
==5251==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-a
==5251==    by 0x140C60: lalloc (alloc.c:246)
==5251==    by 0x154893: ins_char_bytes (change.c:1099)
==5251==    by 0x154BF4: ins_char (change.c:1014)
==5251==    by 0x17DBBC: mb_replace_pop_ins (edit.c:3115)
==5251==    by 0x17DD54: replace_pop_ins (edit.c:3089)
==5251==    by 0x17DEF5: replace_do_bs (edit.c:3214)
==5251==    by 0x13D962: ins_bs (edit.c:4188)
==5251==    by 0x181717: edit (edit.c:958)
==5251==    by 0x22F599: invoke_edit.isra.1 (normal.c:7035)
==5251==    by 0x2317D1: n_opencmd (normal.c:6279)
==5251==    by 0x2317D1: nv_open (normal.c:7416)
==5251==    by 0x2385B4: normal_cmd (normal.c:939)
==5251==
==5251==
==5251== HEAP SUMMARY:
==5251==     in use at exit: 1,496,302 bytes in 1,299 blocks
==5251==   total heap usage: 3,039 allocs, 1,740 frees, 4,821,241 bytes all
==5251==
==5251== LEAK SUMMARY:
==5251==    definitely lost: 0 bytes in 0 blocks
==5251==    indirectly lost: 0 bytes in 0 blocks
==5251==      possibly lost: 2,058 bytes in 258 blocks
==5251==    still reachable: 1,494,244 bytes in 1,041 blocks
==5251==         suppressed: 0 bytes in 0 blocks
==5251== Rerun with --leak-check=full to see details of leaked memory
==5251==
==5251== For counts of detected and suppressed errors, rerun with: -v
==5251== ERROR SUMMARY: 4 errors from 1 contexts (suppressed: 0 from 0)
```

Attachment

poc24

Impact

This may result in corruption of sensitive information, a crash, or code execution among other things.

CVE
CVE-2022-2207
(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Registry
Other

Affected Version
8.2.5151

Visibility
Public

Status
Fixed

Found by

xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 1,085 times.

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

We have contacted a member of the vim team and are waiting to hear back 5 months ago

Bram Moolenaar 5 months ago Maintainer

I can reproduce the problem, but the POC is too messy to use for a test. It sets lots of options in a rather random way, hard to say what matters.

Bram Moolenaar validated this vulnerability 5 months ago

xikhud 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 8.2.5162

Bram Moolenaar marked this as fixed in 8.2 with commit 0971c7 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us