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

0

Valid Reported on Jun 29th 2022

Description

Heap-based buffer overflow in function `inc` at misc2.c:344

Version

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

Proof of Concept

```
guest@elk:~/trung$ valgrind ./vim_latest/src/vim  -u NONE -i NONE -n -m -X
==6151== Memcheck, a memory error detector
==6151== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==6151== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright infc
==6151== Command: ./vim_latest/src/vim -u NONE -i NONE -n -m -X -Z -e -s -S
==6151==
==6151== Invalid read of size 1
==6151==    at 0x223E25: inc (misc2.c:344)
==6151==    by 0x2340DB: nv_put_opt (normal.c:7372)
==6151==    by 0x238604: normal_cmd (normal.c:939)
==6151==    by 0x1B674C: exec_normal (ex_docmd.c:8807)
==6151==    by 0x1B69AF: ex_normal (ex_docmd.c:8693)
==6151==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==6151==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==6151==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==6151==    by 0x2ACF43: do_source (scriptfile.c:1801)
==6151==    by 0x2ACF43: cmd_source (scriptfile.c:1174)
==6151==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==6151==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==6151==    by 0x380B1F: exe_commands (main.c:3133)
```

```
==6151==    by 0x380B1F: vim_main2 (main.c:780)
==6151==    by 0x13F6DC: main (main.c:432)
==6151==  Address 0x5e5f794 is 4 bytes after a block of size 4,096 alloc'd
==6151==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-a
==6151==    by 0x140C70: lalloc (alloc.c:246)
==6151==    by 0x3812AA: mf_alloc_bhdr.isra.3 (memfile.c:884)
==6151==    by 0x382086: mf_new (memfile.c:375)
==6151==    by 0x21480F: ml_new_data (memline.c:4080)
==6151==    by 0x2176CC: ml_open (memline.c:394)
==6151==    by 0x150EB4: open_buffer (buffer.c:186)
==6151==    by 0x380429: create_windows (main.c:2902)
==6151==    by 0x380429: vim_main2 (main.c:711)
==6151==    by 0x13F6DC: main (main.c:432)
==6151==
==6151==
==6151== HEAP SUMMARY:
==6151==     in use at exit: 69,739 bytes in 405 blocks
==6151==   total heap usage: 1,204 allocs, 799 frees, 261,409 bytes allocat
==6151==
==6151== LEAK SUMMARY:
==6151==    definitely lost: 0 bytes in 0 blocks
==6151==    indirectly lost: 0 bytes in 0 blocks
==6151==      possibly lost: 0 bytes in 0 blocks
==6151==    still reachable: 69,739 bytes in 405 blocks
==6151==         suppressed: 0 bytes in 0 blocks
==6151== Rerun with --leak-check=full to see details of leaked memory
==6151==
==6151== For counts of detected and suppressed errors, rerun with: -v
==6151== ERROR SUMMARY: 1 errors from 1 contexts (suppressed: 0 from 0)
```

Attachment

poc80min3

Impact

This may result in corruption of sensitive information, a crash, or code execu
things.

CVE
CVE-2022-2264

(Published)

Vulnerability Type
CWE-122: Heap-based Buffer Overflow

Severity
High (7.8)

Registry
Other

Affected Version
8.2.5164

Visibility
Public

Status
Fixed

Found by

xikhud
@acquykhud
legend

Fixed by

Bram Moolenaar
@brammool
maintainer

This report was seen 729 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 back 5 months ago

Bram Moolenaar validated this vulnerability 5 months ago

I can reproduce it.

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 9.0.0011

Bram Moolenaar marked this as fixed in **9.0** with commit **d25f00** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation

terms

privacy policy

Chat with us