huntr

Out-of-bound read in function msg_outtrans_special in vim/vim

0

✓ Valid Reported on Jun 27th 2022

Description

Out-of-bound read in function `msg_outtrans_special` at message.c:1716

Version

```
commit c101abff4c6756db4f5e740fde289decb9452efa (HEAD -> master, tag: v8.2.
```

Proof of Concept

```
guest@elk:~/trung$ valgrind ./vim_latest/src/vim -u NONE -i NONE -n -m -X -
==23509== Memcheck, a memory error detector
==23509== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==23509== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright inf
==23509== Command: ./vim_latest/src/vim -u NONE -i NONE -n -m -X -Z -e -s -
==23509==
==23509== Invalid read of size 1
==23509==    at 0x385F02: msg_outtrans_special (message.c:1716)
==23509==    by 0x21D258: show_menus_recursive (menu.c:1214)
==23509==    by 0x21D244: show_menus_recursive (menu.c:1230)
==23509==    by 0x21D244: show_menus_recursive (menu.c:1230)
==23509==    by 0x21D40B: show_menus (menu.c:1153)
==23509==    by 0x21E4A9: ex_menu (menu.c:284)
==23509==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==23509==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==23509==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==23509==    by 0x2ACF43: do_source (scriptfile.c:1801)
```

```
==23509==    by 0x2ACF43: cmd_source (scriptfile.c:1174)
==23509==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==23509==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)

==23509==    by 0x380B1F: exe_commands (main.c:3133)
==23509==    by 0x380B1F: vim_main2 (main.c:780)
==23509==    by 0x13F6DC: main (main.c:432)
==23509==  Address 0x5e649d4 is 0 bytes after a block of size 4 alloc'd
==23509==    at 0x4C31B0F: malloc (in /usr/lib/valgrind/vgpreload_memcheck-
==23509==    by 0x140C70: lalloc (alloc.c:246)
==23509==    by 0x2DA5D9: vim_strsave (strings.c:27)
==23509==    by 0x21DD25: add_menu_path (menu.c:742)
==23509==    by 0x21E71A: ex_menu (menu.c:380)
==23509==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==23509==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==23509==    by 0x2ABF50: do_source_ext (scriptfile.c:1674)
==23509==    by 0x2ACF43: do_source (scriptfile.c:1801)
==23509==    by 0x2ACF43: cmd_source (scriptfile.c:1174)
==23509==    by 0x1BB2CD: do_one_cmd (ex_docmd.c:2570)
==23509==    by 0x1BB2CD: do_cmdline (ex_docmd.c:992)
==23509==    by 0x380B1F: exe_commands (main.c:3133)
==23509==    by 0x380B1F: vim_main2 (main.c:780)
==23509==    by 0x13F6DC: main (main.c:432)
==23509==
==23509==
==23509== HEAP SUMMARY:
==23509==     in use at exit: 67,943 bytes in 368 blocks
==23509==   total heap usage: 1,012 allocs, 644 frees, 200,797 bytes alloca
==23509==
==23509== LEAK SUMMARY:
==23509==    definitely lost: 0 bytes in 0 blocks
==23509==    indirectly lost: 0 bytes in 0 blocks
==23509==      possibly lost: 0 bytes in 0 blocks
==23509==    still reachable: 67,943 bytes in 368 blocks
==23509==         suppressed: 0 bytes in 0 blocks
==23509== Rerun with --leak-check=full to see details of leaked memory
==23509==
==23509== For counts of detected and suppressed errors, rerun with: -v
==23509== ERROR SUMMARY: 1 errors from 1 contexts (suppressed
```

Attachment

poc4min2

Impact

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

CVE
CVE-2022-2257
(Published)

Vulnerability Type
CWE-125: Out-of-bounds Read

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 707 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. The POC is simple.

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 9.0.0009

Bram Moolenaar marked this as fixed in **9.0** with commit **083692** 5 months ago

Bram Moolenaar has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation