



# CVE-2022-2522

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2022-2522
<b>State</b>	PUBLIC
<b>Assigner</b>	security@huntr.dev
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-07-25 14:15:00 UTC
<b>Updated</b>	2023-05-03 12:16:00 UTC
<b>Description</b>	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0061.

## Risk And Classification

**Problem Types:** CWE-122

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Vim	Vim	All	All	All	All

## References

Reference	Source	Link
Heap-based Buffer Overflow in function ins_compl_infercase_gettext() vulnerability found in vim	MISC	<a href="https://www.huntr.dev">huntr.dev</a>
patch 9.0.0060: accessing uninitialized memory when completing long line · vim/vim@b9e7173 · GitHub	MISC	<a href="https://github.com">github.com</a>
Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security	GENTOO	<a href="https://security.gentoo.org">security.gentoo.org</a>
Heap-based Buffer Overflow in function ins_compl_infercase_gettext() vulnerability found in vim	CONFIRM	<a href="https://www.huntr.dev">huntr.dev</a>
patch 9.0.0061: ml_get error with nested autocommand · vim/vim@5fa9f23 · GitHub	MISC	<a href="https://github.com">github.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[182805](#) Debian Security Update for vim (CVE-2022-2522)

[199672](#) Ubuntu Security Notification for Vim Vulnerabilities (USN-6302-1)

354478 Amazon Linux Security Advisory for vim : ALAS2022-2022-131
354497 Amazon Linux Security Advisory for vim : ALAS2022-2022-155
354585 Amazon Linux Security Advisory for vim : ALAS-2022-155
354794 Amazon Linux Security Advisory for vim : ALAS2-2023-1975
354870 Amazon Linux Security Advisory for vim : ALAS-2023-1716
355135 Amazon Linux Security Advisory for vim : ALAS2023-2023-098
672105 EulerOS Security Update for vim (EulerOS-SA-2022-2307)
672124 EulerOS Security Update for vim (EulerOS-SA-2022-2336)
672284 EulerOS Security Update for vim (EulerOS-SA-2022-2671)
672300 EulerOS Security Update for vim (EulerOS-SA-2022-2703)
710718 Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202305-16)
752573 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:3229-1)
753066 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:4619-1)
902561 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10323)
902562 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10321)
903765 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10323-1)
903940 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10321-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**