



CVE-2022-0392

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2022-0392
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-28 22:15:00 UTC
Updated	2022-11-29 22:12:00 UTC
Description	Heap-based Buffer Overflow in GitHub repository vim prior to 8.2.

Risk And Classification

Problem Types: CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Vim	Vim	All	All	All	All

References

Reference	Source	Link
About the security content of macOS Monterey 12.6 - Apple Support	CONFIRM	support.a
Full Disclosure: APPLE-SA-2022-10-27-5 Additional information for APPLE-SA-2022-10-24-2 macOS Ventura 13	FULLDISC	seclists.o
patch 8.2.4218: illegal memory access with bracketed paste in Ex mode · vim/vim@806d037 · GitHub	MISC	github.co
Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security	GENTOO	security.g
About the security content of macOS Ventura 13 - Apple Support	CONFIRM	support.a
Heap-based Buffer Overflow vulnerability found in vim	CONFIRM	huntr.dev
Full Disclosure: APPLE-SA-2022-10-27-7 Additional information for APPLE-SA-2022-09-12-4 macOS Monterey 12.6	FULLDISC	seclists.o
Full Disclosure: APPLE-SA-2022-10-24-2 macOS Ventura 13	FULLDISC	seclists.o
[SECURITY] [DLA 3204-1] vim security update	MLIST	lists.debi
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159708](#) Oracle Enterprise Linux Security Update for vim (ELSA-2022-0894)

[181246](#) Debian Security Update for vim (DLA 3204-1)

[184885](#) Debian Security Update for vim (CVE-2022-0392)

[199104](#) Ubuntu Security Notification for Vim Vulnerabilities (USN-5801-1)

[240146](#) Red Hat Update for vim (RHSA-2022:0894)

[353954](#) Amazon Linux Security Advisory for vim : ALAS-2022-1597

[354421](#) Amazon Linux Security Advisory for vim : ALAS2022-2022-023

[354497](#) Amazon Linux Security Advisory for vim : ALAS2022-2022-155

[354585](#) Amazon Linux Security Advisory for vim : ALAS-2022-155

[355135](#) Amazon Linux Security Advisory for vim : ALAS2023-2023-098

[376429](#) Vim Heap-based buffer Overflow Vulnerability

[500731](#) Alpine Linux Security Update for vim

[502238](#) Alpine Linux Security Update for vim

[504504](#) Alpine Linux Security Update for vim

[671458](#) EulerOS Security Update for vim (EulerOS-SA-2022-1441)

[671465](#) EulerOS Security Update for vim (EulerOS-SA-2022-1462)

[671633](#) EulerOS Security Update for vim (EulerOS-SA-2022-1669)

[671639](#) EulerOS Security Update for vim (EulerOS-SA-2022-1655)

[671882](#) EulerOS Security Update for vim (EulerOS-SA-2022-1953)

[710607](#) Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202208-32)

[752246](#) SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:2102-1)

[753066](#) SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:4619-1)

[900622](#) Common Base Linux Mariner (CBL-Mariner) Security Update for vim (8353)

[901217](#) Common Base Linux Mariner (CBL-Mariner) Security Update for vim (8365-1)

[940466](#) AlmaLinux Security Update for vim (ALSA-2022:0894)

[960690](#) Rockv Linux Security Update for vim (RLSA-2022:0894)

© [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](#)