



CVE-2022-1968

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

Summary

CVE	CVE-2022-1968
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-02 14:15:00 UTC
Updated	2023-05-03 12:15:00 UTC
Description	Use After Free in GitHub repository vim/vim prior to 8.2.

Risk And Classification

Problem Types: CWE-416

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
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Vim	Vim	All	All	All	All

References

Reference	Source	Link
Full Disclosure: APPLE-SA-2022-10-27-5 Additional information for APPLE-SA-2022-10-24-2 macOS Ventura 13	FULLDISC	seclists.org
[SECURITY] [DLA 3182-1] vim security update	MLIST	lists.debian.org
Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security	GENTOO	security.gentoo.org
Use After Free in function utf_ptr2char vulnerability found in vim	CONFIRM	huntr.dev
About the security content of macOS Ventura 13 - Apple Support	CONFIRM	support.apple.com
Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security	GENTOO	security.gentoo.org
patch 8.2.5050: using freed memory when searching for pattern in path · vim/vim@409510c · GitHub	MISC	github.com
Full Disclosure: APPLE-SA-2022-10-24-2 macOS Ventura 13	FULLDISC	seclists.org
[SECURITY] [DLA 3053-1] vim security update	MLIST	lists.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179379 Debian Security Update for vim (DLA 3053-1)
181198 Debian Security Update for vim (DLA 3182-1)
182201 Debian Security Update for vim (CVE-2022-1968)
199271 Ubuntu Security Notification for Vim Vulnerabilities (USN-5995-1)
354009 Amazon Linux Security Advisory for vim : ALAS2-2022-1829
354033 Amazon Linux Security Advisory for vim : ALAS-2022-1628
354356 Amazon Linux Security Advisory for vim : ALAS2022-2022-116
354497 Amazon Linux Security Advisory for vim : ALAS2022-2022-155
354585 Amazon Linux Security Advisory for vim : ALAS-2022-155
355073 Amazon Linux Security Advisory for vim : AL2012-2023-397
355135 Amazon Linux Security Advisory for vim : ALAS2023-2023-098
672048 EulerOS Security Update for vim (EulerOS-SA-2022-2282)
672056 EulerOS Security Update for vim (EulerOS-SA-2022-2263)
672072 EulerOS Security Update for vim (EulerOS-SA-2022-2250)
672076 EulerOS Security Update for vim (EulerOS-SA-2022-2237)
672105 EulerOS Security Update for vim (EulerOS-SA-2022-2307)
672124 EulerOS Security Update for vim (EulerOS-SA-2022-2336)
672223 EulerOS Security Update for vim (EulerOS-SA-2022-2639)
710607 Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202208-32)
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)

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](#)