



CVE-2022-2207

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

Summary

CVE	CVE-2022-2207
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-27 12:15:00 UTC
Updated	2023-11-07 03:46:00 UTC
Description	Heap-based Buffer Overflow in GitHub repository vim/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	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Vim	Vim	All	All	All	All

References

Reference	Source	Link	Ta
Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 36 Update: vim-8.2.5172-1.fc36 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security	GENTOO	security.gentoo.org	
Heap-based buffer overflow in function ins_bs vulnerability found in vim	CONFIRM	huntr.dev	
patch 8.2.5162: reading before the start of the line with BS in Repla... · vim/vim@0971c7a · GitHub	MISC	github.com	
[SECURITY] Fedora 35 Update: vim-8.2.5172-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 35 Update: vim-8.2.5172-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 36 Update: vim-8.2.5172-1.fc36 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

184678 Debian Security Update for vim (CVE-2022-2207)
199293 Ubuntu Security Notification for Vim Vulnerabilities (USN-6026-1)
282876 Fedora Security Update for vim (FEDORA-2022-719f3ec21b)
282892 Fedora Security Update for vim (FEDORA-2022-bb7f3cacbf)
296086 Oracle Solaris 11.4 Support Repository Update (SRU) 51.132.1 Missing (CPUOCT2022)
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
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)
672146 EulerOS Security Update for vim (EulerOS-SA-2022-2451)
672152 EulerOS Security Update for vim (EulerOS-SA-2022-2436)
672157 EulerOS Security Update for vim (EulerOS-SA-2022-2423)
672191 EulerOS Security Update for vim (EulerOS-SA-2022-2483)
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)
902402 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9983)
902405 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9977)
902497 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9983-1)
902545 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9977-1)

© [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](#)