



# CVE-2022-2845

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2022-2845
<b>State</b>	PUBLIC
<b>Assigner</b>	security@huntr.dev
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-17 15:15:00 UTC
<b>Updated</b>	2023-07-10 16:15:00 UTC
<b>Description</b>	Improper Validation of Specified Quantity in Input in GitHub repository vim/vim prior to 9.0.0218.

## Risk And Classification

**Problem Types:** CWE-1284

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Application	<a href="#">Vim</a>	<a href="#">Vim</a>	All	All	All	All

## References

Reference	Source	Link	Tags
patch 9.0.0218: reading before the start of the line · vim/vim@e98c88c · GitHub	MISC	<a href="#">github.com</a>	
[SECURITY] Fedora 35 Update: vim-9.0.246-1.fc35 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproject.org</a>	
Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>	
[SECURITY] Fedora 35 Update: vim-9.0.246-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
Buffer Over-read in function utf_head_off vulnerability found in vim	CONFIRM	<a href="#">huntr.dev</a>	
[SECURITY] Fedora 37 Update: vim-9.0.412-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="#">lists.fedoraproject.org</a>	
[SECURITY] Fedora 37 Update: vim-9.0.412-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

182733	Debian Security Update for vim (CVE-2022-2845)
199271	Ubuntu Security Notification for Vim Vulnerabilities (USN-5995-1)
283076	Fedora Security Update for vim (FEDORA-2022-3b33d04743)
354087	Amazon Linux Security Advisory for vim : ALAS2-2022-1868
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
355135	Amazon Linux Security Advisory for vim : ALAS2023-2023-098
672146	EulerOS Security Update for vim (EulerOS-SA-2022-2451)
672191	EulerOS Security Update for vim (EulerOS-SA-2022-2483)
672284	EulerOS Security Update for vim (EulerOS-SA-2022-2671)
672300	EulerOS Security Update for vim (EulerOS-SA-2022-2703)
672330	EulerOS Security Update for vim (EulerOS-SA-2022-2783)
672395	EulerOS Security Update for vim (EulerOS-SA-2022-2748)
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)
902758	Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10581)
902762	Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10569)
903927	Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10569-1)
903991	Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10581-1)

© [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](#)