



# CVE-2023-2426

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

## Summary

<b>CVE</b>	CVE-2023-2426
<b>State</b>	PUBLIC
<b>Assigner</b>	security@huntr.dev
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-04-29 22:15:00 UTC
<b>Updated</b>	2023-12-23 07:15:00 UTC
<b>Description</b>	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 9.0.1499.

## Risk And Classification

**Problem Types:** CWE-823

## 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	Tags
[SECURITY] Fedora 38 Update: vim-9.0.1562-1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
patch 9.0.1499: using uninitialized memory with fuzzy matching · vim/vim@caf642c · GitHub	MISC	<a href="https://github.com">github.com</a>	
[SECURITY] Fedora 38 Update: vim-9.0.1562-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
huntr – Security Bounties for any GitHub repository	CONFIRM	<a href="https://huntr.dev">huntr.dev</a>	
About the security content of macOS Monterey 12.6.8 - Apple Support		<a href="https://support.apple.com">support.apple.com</a>	
[SECURITY] Fedora 37 Update: vim-9.0.1562-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
About the security content of macOS Big Sur 11.7.9 - Apple Support		<a href="https://support.apple.com">support.apple.com</a>	
[SECURITY] Fedora 37 Update: vim-9.0.1562-1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy OID Mappings

<a href="#">182057</a> Debian Security Update for vim (CVE-2023-2426)
<a href="#">199407</a> Ubuntu Security Notification for Vim Vulnerabilities (USN-6154-1)
<a href="#">283993</a> Fedora Security Update for vim (FEDORA-2023-99d2eaac80)
<a href="#">284110</a> Fedora Security Update for vim (FEDORA-2023-d6baa1d93e)
<a href="#">355429</a> Amazon Linux Security Advisory for vim : ALAS-2023-1761
<a href="#">673212</a> EulerOS Security Update for vim (EulerOS-SA-2023-2371)
<a href="#">673216</a> EulerOS Security Update for vim (EulerOS-SA-2023-2397)
<a href="#">673265</a> EulerOS Security Update for vim (EulerOS-SA-2023-2630)
<a href="#">673282</a> EulerOS Security Update for vim (EulerOS-SA-2023-2600)
<a href="#">673492</a> EulerOS Security Update for vim (EulerOS-SA-2023-2714)
<a href="#">674067</a> EulerOS Security Update for vim (EulerOS-SA-2023-2672)
<a href="#">754268</a> SUSE Enterprise Linux Security Update for vim (SUSE-SU-2023:2640-1)
<a href="#">906888</a> Common Base Linux Mariner (CBL-Mariner) Security Update for vim (26403-1)
<a href="#">906895</a> Common Base Linux Mariner (CBL-Mariner) Security Update for vim (26394-1)

© [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](#)**