



# CVE-2023-48235

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

## Summary

<b>CVE</b>	CVE-2023-48235
<b>State</b>	PUBLISHED
<b>Assigner</b>	Unknown
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-11-16 23:15:00 UTC
<b>Updated</b>	2024-01-25 21:33:00 UTC
<b>Description</b>	Description unavailable.

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	39	All	All	All
Application	<a href="#">Vim</a>	<a href="#">Vim</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - [vim-security] several minor security issues in Vim v9.0.2106-v9.0.2112		<a href="#">www.openwall.com</a>	
[SECURITY] Fedora 37 Update: vim-9.0.2120-1.fc37 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	Mailir
[SECURITY] Fedora 39 Update: vim-9.0.2120-1.fc39 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	Mailir
[SECURITY] Fedora 38 Update: vim-9.0.2120-1.fc38 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>	Mailir
overflow in ex address parsing · Advisory · vim/vim · GitHub		<a href="#">github.com</a>	
CVE-2023-48235 Vim Vulnerability in NetApp Products   NetApp Product Security		<a href="#">security.netapp.com</a>	Third
patch 9.0.2110: [security]: overflow in ex address parsing · vim/vim@060623e · GitHub		<a href="#">github.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">200016</a> Ubuntu Security Notification for Vim Vulnerabilities (USN-6557-1)
<a href="#">284764</a> Fedora Security Update for vim (FEDORA-2023-ce3f7d4818)
<a href="#">284765</a> Fedora Security Update for vim (FEDORA-2023-eec2cdb7ed)
<a href="#">285130</a> Fedora Security Update for vim (FEDORA-2023-45cf2b4014)
<a href="#">356776</a> Amazon Linux Security Advisory for vim : ALAS2-2023-2353
<a href="#">356909</a> Amazon Linux Security Advisory for vim : ALAS2023-2023-447
<a href="#">357186</a> Amazon Linux Security Advisory for vim : AL2012-2024-485
<a href="#">673345</a> EulerOS Security Update for vim (EulerOS-SA-2024-1130)
<a href="#">673552</a> EulerOS Security Update for vim (EulerOS-SA-2024-1099)
<a href="#">673740</a> EulerOS Security Update for vim (EulerOS-SA-2024-1075)
<a href="#">673930</a> EulerOS Security Update for vim (EulerOS-SA-2024-1189)
<a href="#">673976</a> EulerOS Security Update for vim (EulerOS-SA-2024-1209)
<a href="#">674064</a> EulerOS Security Update for vim (EulerOS-SA-2024-1114)
<a href="#">755920</a> SUSE Enterprise Linux Security Update for vim (SUSE-SU-2024:0783-1)
<a href="#">755972</a> SUSE Enterprise Linux Security Update for vim (SUSE-SU-2024:0871-1)
<a href="#">907668</a> Common Base Linux Mariner (CBL-Mariner) Security Update for vim (32026-1)

© [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](#)