



CVE-2023-5535

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2023-5535 |
| State | PUBLIC |
| Assigner | security@huntr.dev |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-10-11 20:15:00 UTC |
| Updated | 2023-11-15 02:31:00 UTC |
| Description | Use After Free in GitHub repository vim/vim prior to v9.0.2010. |

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 37 | All | All | All |
| Operating System | Fedoraproject | Fedora | 38 | All | All | All |
| Operating System | Fedoraproject | Fedora | 39 | All | All | All |
| Application | Vim | Vim | All | All | All | All |

References

| Reference | Source | Link | Ta |
|--|---------|---|-----|
| [SECURITY] Fedora 38 Update: vim-9.0.2048-1.fc38 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| [SECURITY] Fedora 39 Update: vim-9.0.2048-1.fc39 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| [SECURITY] Fedora 37 Update: vim-9.0.2048-1.fc37 - package-announce - Fedora Mailing-Lists | MISC | lists.fedoraproject.org | |
| patch 9.0.2010: [security] use-after-free from buf_contents_changed() · vim/vim@41e6f7d · GitHub | MISC | github.com | |
| huntr – Security Bounties for any GitHub repository | MISC | huntr.dev | |
| CVE Program record | CVE.ORG | www.cve.org | car |
| NVD vulnerability detail | NVD | nvd.nist.gov | car |

No vendor comments have been submitted for this CVE.

Legacy OID Mappings

| |
|--|
| 199867 Ubuntu Security Notification for Vim Vulnerabilities (USN-6452-1) |
| 284650 Fedora Security Update for vim (FEDORA-2023-e9c71abc95) |
| 284651 Fedora Security Update for vim (FEDORA-2023-6c84e57fab) |
| 285183 Fedora Security Update for vim (FEDORA-2023-1976197889) |
| 356575 Amazon Linux Security Advisory for vim : ALAS2-2023-2319 |
| 356632 Amazon Linux Security Advisory for vim : ALAS2023-2023-403 |
| 356783 Amazon Linux Security Advisory for vim : ALAS-2023-1893 |
| 357186 Amazon Linux Security Advisory for vim : AL2012-2024-485 |
| 503545 Alpine Linux Security Update for vim |
| 505960 Alpine Linux Security Update for vim |
| 673552 EulerOS Security Update for vim (EulerOS-SA-2024-1099) |
| 673558 EulerOS Security Update for vim (EulerOS-SA-2023-3288) |
| 673740 EulerOS Security Update for vim (EulerOS-SA-2024-1075) |
| 673745 EulerOS Security Update for vim (EulerOS-SA-2023-3320) |
| 673779 EulerOS Security Update for vim (EulerOS-SA-2023-3260) |
| 673841 EulerOS Security Update for vim (EulerOS-SA-2023-3352) |
| 755336 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2023:4560-1) |
| 755339 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2023:4557-1) |
| 755354 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2023:4587-1) |
| 907430 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (31499-1) |

© [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](#)