



CVE-2022-2288

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2022-2288 |
| State | PUBLIC |
| Assigner | security@huntr.dev |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-07-03 13:15:00 UTC |
| Updated | 2023-11-07 03:46:00 UTC |
| Description | Out-of-bounds Write in GitHub repository vim/vim prior to 9.0. |

Risk And Classification

Problem Types: CWE-787

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 |
|---|---------|---|
| [SECURITY] Fedora 36 Update: vim-9.0.049-1.fc36 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| patch 9.0.0025: accessing beyond allocated memory with the cmdline wi... · vim/vim@c6fdb15 · GitHub | MISC | github.com |
| Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security | GENTOO | security.gentoo.org |
| Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security | GENTOO | security.gentoo.org |
| huntr – Security Bounties for any GitHub repository | CONFIRM | huntr.dev |
| [SECURITY] Fedora 36 Update: vim-9.0.049-1.fc36 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| [SECURITY] Fedora 35 Update: vim-9.0.049-1.fc35 - package-announce - Fedora Mailing-Lists | | lists.fedoraproject.org |
| [SECURITY] Fedora 35 Update: vim-9.0.049-1.fc35 - package-announce - Fedora Mailing-Lists | FEDORA | lists.fedoraproject.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| | |
|--------|---|
| 183113 | Debian Security Update for vim (CVE-2022-2288) |
| 282933 | Fedora Security Update for vim (FEDORA-2022-b06fbea2c7) |
| 282957 | Fedora Security Update for vim (FEDORA-2022-9d7a58e376) |
| 354085 | Amazon Linux Security Advisory for vim : ALAS-2022-1639 |
| 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 |
| 502803 | Alpine Linux Security Update for vim |
| 710607 | Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202208-32) |
| 710718 | Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202305-16) |
| 902439 | Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10051) |
| 902446 | Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10060) |
| 902635 | Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10060-1) |
| 902691 | Common Base Linux Mariner (CBL-Mariner) Security Update for vim (10051-1) |

© [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](#)