



CVE-2021-3872

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

Summary

CVE	CVE-2021-3872
State	PUBLIC
Assigner	security@huntr.dev
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-19 13:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	vim is vulnerable to Heap-based Buffer Overflow

Risk And Classification

Problem Types: CWE-122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Vim	Vim	All	All	All	All

References

Reference	Source	Link	Tags
Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security	GENTOO	security.gentoo.org	
[SECURITY] Fedora 33 Update: vim-8.2.3512-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
huntr: Disclose & Fix Security Vulnerabilities in Open Source	CONFIRM	huntr.dev	
[SECURITY] Fedora 35 Update: vim-8.2.3512-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] Fedora 33 Update: vim-8.2.3512-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
[SECURITY] [DLA 2947-1] vim security update	MLIST	lists.debian.org	
patch 8.2.3487: illegal memory access if buffer name is very long · vim/vim@826bfe4 · GitHub	MISC	github.com	
[SECURITY] Fedora 35 Update: vim-8.2.3512-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159623 Oracle Enterprise Linux Security Update for vim (ELSA-2022-0366)
179126 Debian Security Update for vim (DLA 2947-1)
184373 Debian Security Update for vim (CVE-2021-3872)
198571 Ubuntu Security Notification for Vim Vulnerabilities (USN-5147-1)
240055 Red Hat Update for vim (RHSA-2022:0366)
282009 Fedora Security Update for vim (FEDORA-2021-84f4cf3244)
296061 Oracle Solaris 11.4 Support Repository Update (SRU) 42.113.1 Missing (CPUJAN2022)
353078 Amazon Linux Security Advisory for vim : ALAS2-2021-1728
354402 Amazon Linux Security Advisory for vim : ALAS2022-2021-001
377370 Alibaba Cloud Linux Security Update for vim (ALINUX3-SA-2022:0011)
671163 EulerOS Security Update for vim (EulerOS-SA-2021-2817)
671183 EulerOS Security Update for vim (EulerOS-SA-2021-2937)
671206 EulerOS Security Update for vim (EulerOS-SA-2022-1040)
671215 EulerOS Security Update for vim (EulerOS-SA-2022-1020)
671261 EulerOS Security Update for vim (EulerOS-SA-2022-1193)
671281 EulerOS Security Update for vim (EulerOS-SA-2022-1236)
671322 EulerOS Security Update for vim (EulerOS-SA-2022-1217)
710607 Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202208-32)
751791 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:0736-1)
751809 OpenSUSE Security Update for vim (openSUSE-SU-2022:0736-1)
752246 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:2102-1)
753066 SUSE Enterprise Linux Security Update for vim (SUSE-SU-2022:4619-1)
900367 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (6028)
940444 AlmaLinux Security Update for vim (ALSA-2022:0366)
960721 Rocky Linux Security Update for vim (RLSA-2022:0366)

© [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](#)