



CVE-2022-1619

Published on: Not Yet Published

Last Modified on: 05/03/2023 12:15:00 PM UTC

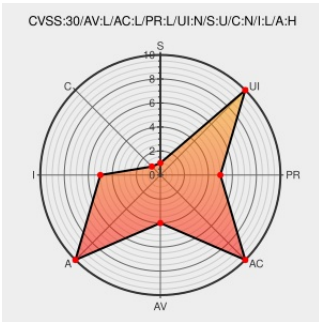
CVE-2022-1619 - advisory for b3200483-624e-4c76-a070-e246f62a7450

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Macos** from **Apple** contain the following vulnerability:

Heap-based Buffer Overflow in function `cmdline_erase_chars` in GitHub repository `vim/vim` prior to 8.2.4899. This vulnerabilities are capable of crashing software, modify memory, and possible remote execution

CVE-2022-1619 has been assigned by security@huntr.dev to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **vim** - **vim/vim** version < 8.2.4899

CVSS3 Score: **7.8 - HIGH**






Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] [DLA 3011-1] vim security update	lists.debian.org text/html	@ MLIST [debian-lts-announce] 20220516 [SECURITY] [DLA 3011-1] vim security update

Full Disclosure: APPLE-SA-2022-10-27-5 Additional information for APPLE-SA-2022-10-24-2 macOS Ventura 13	seclists.org text/html	 FULLDISC 20221030 APPLE-SA-2022-10-27-5 Additional information for APPLE-SA-2022-10-24-2 macOS Ventura 13
[SECURITY] Fedora 36 Update: vim-8.2.4927-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2022-e92c3ce170
Vim, gVim: Multiple Vulnerabilities (GLSA 202208-32) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202208-32
About the security content of macOS Ventura 13 - Apple Support	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT213488
Vim, gVim: Multiple Vulnerabilities (GLSA 202305-16) — Gentoo security	security.gentoo.org text/html	 GENTOO GLSA-202305-16
[SECURITY] Fedora 34 Update: vim-8.2.4927-1.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2022-8df66cdbef
patch 8.2.4899: with latin1 encoding CTRL-W might go before the cmdline · vim/vim@ef02f16 · GitHub	github.com text/html	 MISC github.com/vim/vim/commit/ef02f16609f0a26ffc6e20263523424980898fe
[SECURITY] Fedora 35 Update: vim-8.2.4927-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2022-f0db3943d9
Full Disclosure: APPLE-SA-2022-10-24-2 macOS Ventura 13	seclists.org text/html	 FULLDISC 20221030 APPLE-SA-2022-10-24-2 macOS Ventura 13
[SECURITY] [DLA 3204-1] vim security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20221124 [SECURITY] [DLA 3204-1] vim security update
Heap-based Buffer Overflow in function cmdline_erase_chars vulnerability found in vim	huntr.dev text/html	 CONFIRM huntr.dev/bounties/b3200483-624e-4c76-a070-e246f62a7450
CVE-2022-1619 Vim Vulnerability in NetApp Products NetApp Product Security	security.netapp.com text/html	 CONFIRM security.netapp.com/advisory/ntap-20220930-0007/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- [179292](#) Debian Security Update for vim (DLA 3011-1)
- [181246](#) Debian Security Update for vim (DLA 3204-1)
- [182593](#) Debian Security Update for vim (CVE-2022-1619)
- [198939](#) Ubuntu Security Notification for Vim Vulnerabilities (USN-5613-1)
- [282670](#) Fedora Security Update for vim (FEDORA-2022-f0db3943d9)
- [282699](#) Fedora Security Update for vim (FEDORA-2022-8df66cdbef)
- [282700](#) Fedora Security Update for vim (FEDORA-2022-e92c3ce170)
- [296082](#) Oracle Solaris 11.4 Support Repository Update (SRU) 48.126.1 Missing (CPUJUL2022)

354009 Amazon Linux Security Advisory for vim : ALAS2-2022-1829

354033 Amazon Linux Security Advisory for vim : ALAS-2022-1628

354356 Amazon Linux Security Advisory for vim : ALAS2022-2022-116

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

502241 Alpine Linux Security Update for vim

671907 EulerOS Security Update for vim (EulerOS-SA-2022-1984)

671935 EulerOS Security Update for vim (EulerOS-SA-2022-2014)

671979 EulerOS Security Update for vim (EulerOS-SA-2022-2173)

671980 EulerOS Security Update for vim (EulerOS-SA-2022-2148)

710607 Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202208-32)

710718 Gentoo Linux Vim, gVim Multiple Vulnerabilities (GLSA 202305-16)

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)

901576 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9710)

901680 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9703)

902085 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9703-1)

902197 Common Base Linux Mariner (CBL-Mariner) Security Update for vim (9710-1)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...






Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	All	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All

Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Netapp	Hci Management Node	-	All	All	All
Application	Netapp	Solidfire	-	All	All	All
Application	Vim	Vim	All	All	All	All
cpe:2.3:o:apple:macos:*:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:34:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:						
cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:						
cpe:2.3:a:netapp:hci_management_node:-:*:*:*:*:*:						
cpe:2.3:a:netapp:solidfire:-:*:*:*:*:*:						
cpe:2.3:a:vim:vim:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @huntrHacktivity	Heap-based Buffer Overflow in github.com/vim/vim (CVE-2022-1619) reported by jieyongma - Patch:... twitter.com/i/web/status/1...	2022-05-07 10:09:20
 @CVEreport	CVE-2022-1619 : Heap-based Buffer Overflow in function cmdline_erase_chars in GitHub repository vim/vim prior to 8.... twitter.com/i/web/status/1...	2022-05-08 09:53:50
 @Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-1619 Heap-based Buffer Overflow in function cmdline_erase_chars in Gith... twitter.com/i/web/status/1...	2022-05-08 10:56:01
 /r/netcve	CVE-2022-1619	2022-05-08 10:38:32
 /r/k12cybersecurity	MS-ISAC CYBERSECURITY ADVISORY - Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution - PATCH: NOW	2022-10-27 12:48:22

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

