



CVE-2022-48337

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

Summary

CVE	CVE-2022-48337
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-02-20 23:15:00 UTC
Updated	2023-11-07 03:56:00 UTC
Description	GNU Emacs through 28.2 allows attackers to execute commands via shell metacharacters in the name of a source-code file

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Gnu	Emacs	All	All	All	All

References

Reference	Source	Link	Ta
[SECURITY] Fedora 37 Update: emacs-28.3-0.rc1.fc37 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 38 Update: emacs-28.3-0.rc1.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
emacs.git - Emacs source repository	MISC	git.savannah.gnu.org	
[SECURITY] [DLA 3416-1] emacs security update	MLIST	lists.debian.org	
[SECURITY] Fedora 38 Update: emacs-28.3-0.rc1.fc38 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org	
Debian -- Security Information -- DSA-5360-1 emacs	DEBIAN	www.debian.org	
[SECURITY] Fedora 37 Update: emacs-28.3-0.rc1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160625](#) Oracle Enterprise Linux Security Update for emacs (ELSA-2023-2626)

[161144](#) Oracle Enterprise Linux Security Update for emacs (ELSA-2023-7083)

[181683](#) Debian Security Update for emacs (DSA 5360-1)

[181775](#) Debian Security Update for emacs (DLA 3416-1)

[182625](#) Debian Security Update for emacs (CVE-2022-48337)

[241452](#) Red Hat Update for emacs (RHSA-2023:2626)

[242440](#) Red Hat Update for emacs (RHSA-2023:7083)

[243011](#) Red Hat Update for emacs (RHSA-2024:1103)

[243088](#) Red Hat Update for emacs (RHSA-2024:1408)

[284551](#) Fedora Security Update for emacs (FEDORA-2023-5763445abe)

[284626](#) Fedora Security Update for emacs (FEDORA-2023-29df561f1d)

[354790](#) Amazon Linux Security Advisory for emacs : ALAS2-2023-1981

[354861](#) Amazon Linux Security Advisory for emacs : ALAS-2023-1712

[355076](#) Amazon Linux Security Advisory for emacs : AL2012-2023-400

[355223](#) Amazon Linux Security Advisory for emacs : ALAS2023-2023-122

[672994](#) EulerOS Security Update for emacs (EulerOS-SA-2023-1840)

[673002](#) EulerOS Security Update for emacs (EulerOS-SA-2023-1865)

[673032](#) EulerOS Security Update for emacs (EulerOS-SA-2023-1950)

[673038](#) EulerOS Security Update for emacs (EulerOS-SA-2023-1972)

[673126](#) EulerOS Security Update for emacs (EulerOS-SA-2023-2288)

[673165](#) EulerOS Security Update for emacs (EulerOS-SA-2023-2264)

[673323](#) EulerOS Security Update for emacs (EulerOS-SA-2023-3124)

[691076](#) Free Berkeley Software Distribution (FreeBSD) Security Update for emacs (a75929bd-b6a4-11ed-bad6-080027f5fec9)

[753737](#) SUSE Enterprise Linux Security Update for emacs (SUSE-SU-2023:0597-1)

[753754](#) SUSE Enterprise Linux Security Update for emacs (SUSE-SU-2023:0675-1)

[905633](#) Common Base Linux Mariner (CBL-Mariner) Security Update for emacs (13702)

[906652](#) Common Base Linux Mariner (CBL-Mariner) Security Update for emacs (13702-3)

[941017](#) AlmaLinux Security Update for emacs (ALSA-2023:2626)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)