



CVE-2023-29491

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-29491
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-14 01:15:00 UTC
Updated	2024-01-31 03:15:00 UTC
Description	ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory cor

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gnu	Ncurses	All	All	All	All

References

Reference	Source	Link
About the security content of macOS Ventura 13.5 - Apple Support	CONFIRM	support.apple.com
About the security content of macOS Monterey 12.6.8 - Apple Support	CONFIRM	support.apple.com
oss-security - ncurses fixes upstream	MISC	www.openwall.com
CVE-2023-29491 GNU Ncurses Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
About the security content of macOS Big Sur 11.7.9 - Apple Support	CONFIRM	support.apple.com
[debian-lts-announce] 20231203 [SECURITY] [DLA 3682-1] ncurses security update		lists.debian.org
oss-security - Re: ncurses fixes upstream	MLIST	www.openwall.com
[SECURITY] Fedora 38 Update: ncurses-6.4-7.20230520.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
oss-security - Re: ncurses fixes upstream	MISC	www.openwall.com
oss-security - RE: [EXTERNAL] Re: ncurses fixes upstream	MLIST	www.openwall.com
ncurses.scripts.mit.edu Git - ncurses.git/commit	MISC	ncurses.scripts.mit.edu
ncurses.scripts.mit.edu Git - ncurses.git/commit		ncurses.scripts.mit.edu
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160932](#) Oracle Enterprise Linux Security Update for ncurses (ELSA-2023-5249)

[161122](#) Oracle Enterprise Linux Security Update for ncurses (ELSA-2023-6698)

[183169](#) Debian Security Update for ncurses (CVE-2023-29491)

[199358](#) Ubuntu Security Notification for ncurses Vulnerabilities (USN-6099-1)

[242067](#) Red Hat Update for ncurses (RHSA-2023:5249)

[242310](#) Red Hat Update for ncurses (RHSA-2023:6698)

[242495](#) Red Hat Update for ncurses (RHSA-2023:7361)

[242748](#) Red Hat Update for ncurses (RHSA-2024:0416)

[284890](#) Fedora Security Update for ncurses (FEDORA-2024-96090dafaf)

[355468](#) Amazon Linux Security Advisory for ncurses : ALAS2023-2023-220

[355538](#) Amazon Linux Security Advisory for ncurses : ALAS2-2023-2096

[355648](#) Amazon Linux Security Advisory for ncurses : ALAS-2023-1778

[378925](#) Alibaba Cloud Linux Security Update for ncurses (ALINUX3-SA-2023:0122)

[503019](#) Alpine Linux Security Update for ncurses

[503020](#) Alpine Linux Security Update for ncurses

[503021](#) Alpine Linux Security Update for ncurses

[505897](#) Alpine Linux Security Update for ncurses

[6000372](#) Debian Security Update for ncurses (DLA 3682-1)

[673221](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-2388)

[673237](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-2362)

[673276](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-2620)

[673292](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-2590)

[673389](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-2699)

[673746](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-3138)

[674004](#) EulerOS Security Update for ncurses (EulerOS-SA-2023-3257)

674004 EulerOS Security Update for ncurses (EulerOS-SA-2023-2657)
753970 SUSE Enterprise Linux Security Update for ncurses (SUSE-SU-2023:2112-1)
754059 SUSE Enterprise Linux Security Update for ncurses (SUSE-SU-2023:2111-1)
906885 Common Base Linux Mariner (CBL-Mariner) Security Update for ncurses (26225-1)
906935 Common Base Linux Mariner (CBL-Mariner) Security Update for ncurses (26241-1)
941257 AlmaLinux Security Update for ncurses (ALSA-2023:5249)
941368 AlmaLinux Security Update for ncurses (ALSA-2023:6698)

© [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](#)