



CVE-2023-43641

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

Summary

CVE	CVE-2023-43641
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-09 22:15:00 UTC
Updated	2023-10-27 17:53:00 UTC
Description	libcue provides an API for parsing and extracting data from CUE sheets. Versions 2.2.1 and prior are vulnerable to out-of-b

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Operating System	Debian	Debian Linux	12.0	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All
Operating System	Fedoraproject	Fedora	39	All	All	All
Application	Lipnitsk	Libcue	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 37 Update: tracker-miners-3.4.5-1.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
libcue: Arbitrary Code Execution (GLSA 202310-10) — Gentoo security	MISC	security.gentoo.org
[SECURITY] Fedora 39 Update: libcue-2.2.1-13.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
[SECURITY] Fedora 38 Update: tracker-miners-3.5.3-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Debian -- Security Information -- DSA-5524-1 libcue	MISC	www.debian.org
[SECURITY] Fedora 38 Update: libcue-2.2.1-13.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Coordinated Disclosure: 1-Click RCE on GNOME (CVE-2023-43641) - The GitHub Blog	MISC	github.blog

[SECURITY] Fedora 37 Update: libcue-2.2.1-13.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
[SECURITY] [DLA 3615-1] libcue security update	MISC	lists.debian.org
Out-of-bounds array access in track_set_index · Advisory · lipnitsk/libcue · GitHub	MISC	github.com
Changelog, CMakeLists.txt: Release 2.3.0 · lipnitsk/libcue@cfb98a0 · GitHub	MISC	github.com
Check that the array index isn't negative. This fixes CVE-2023-43641. · lipnitsk/libcue@fdf72c8 · GitHub	MISC	github.com
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

- [199816](#) Ubuntu Security Notification for CUE Vulnerability (USN-6423-1)
- [199904](#) Ubuntu Security Notification for CUE Vulnerability (USN-6423-2)
- [284601](#) Fedora Security Update for tracker (FEDORA-2023-40044895ce)
- [284602](#) Fedora Security Update for tracker (FEDORA-2023-e8f45c67f5)
- [284609](#) Fedora Security Update for libcue (FEDORA-2023-eec9ce5935)
- [284613](#) Fedora Security Update for libcue (FEDORA-2023-1fe05ac8d9)
- [285205](#) Fedora Security Update for libcue (FEDORA-2023-f4e74a94a2)
- [503376](#) Alpine Linux Security Update for libcue
- [506107](#) Alpine Linux Security Update for libcue
- [6000285](#) Debian Security Update for libcue (DLA 3615-1)
- [6000317](#) Debian Security Update for libcue (DSA 5524-1)
- [691328](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libcue (ae0ee356-6ae1-11ee-bfb6-8c164567ca3c)
- [710771](#) Gentoo Linux libcue Arbitrary Code Execution Vulnerability (GLSA 202310-10)
- [755098](#) SUSE Enterprise Linux Security Update for libcue (SUSE-SU-2023:4090-1)

© 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](#).

Free CVE JSON API cve.report/api

