



CVE-2023-43361

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-43361
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-02 21:15:00 UTC
Updated	2024-01-27 03:15:00 UTC
Description	Buffer Overflow vulnerability in Vorbis-tools v.1.4.2 allows a local attacker to execute arbitrary code and cause a denial of service.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xiph	Vorbis-tools	1.4.2	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 39 Update: vorbis-tools-1.4.2-10.fc39 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
GitHub - xiph/vorbis-tools: Command-line tools for creating and playing Ogg Vorbis files.	MISC	github.com
[SECURITY] Fedora 38 Update: vorbis-tools-1.4.2-9.fc38 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
GitHub - xiph/vorbis: Reference implementation of the Ogg Vorbis audio format.	MISC	github.com
Heap-buffer-overflow on vorbis-tools/oggenc · Issue #41 · xiph/vorbis-tools · GitHub	MISC	github.com
Xiph.org	MISC	xiph.org
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

284887 Fedora Security Update for vorbis (FEDORA-2024-5f8da7c1f1)

285030 Fedora Security Update for vorbis (FEDORA-2024-faff3dd9d6)
356615 Amazon Linux Security Advisory for vorbis-tools : ALAS2023-2023-414
503470 Alpine Linux Security Update for vorbis-tools
506265 Alpine Linux Security Update for vorbis-tools
691347 Free Berkeley Software Distribution (FreeBSD) Security Update for vorbistools (a1a1f81c-7c13-11ee-bcf1-f8b156b6dcc8)
755170 SUSE Enterprise Linux Security Update for vorbis-tools (SUSE-SU-2023:4218-1)
755185 SUSE Enterprise Linux Security Update for vorbis-tools (SUSE-SU-2023:4251-1)

© [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](#)

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