



CVE-2017-12562

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

Summary

CVE	CVE-2017-12562
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-05 17:29:00 UTC
Updated	2022-12-02 22:58:00 UTC
Description	Heap-based Buffer Overflow in the psf_binheader_writef function in common.c in libsndfile through 1.0.28 allows remote att

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libsndfile Project	Libsndfile	1.0.28	All	All	All
Application	Libsndfile Project	Libsndfile	1.0.28	All	All	All

References

Reference	Source	Link
Heap buffer overflows in `psf_binheader_writef` in 1.0.28 and later · Issue #292 · erikd/libsndfile · GitHub	CONFIRM	github.com
[SECURITY] [DLA 3058-1] libsndfile security update	MLIST	lists.debian.org
libsndfile: Multiple vulnerabilities (GLSA 201811-23) — Gentoo security	GENTOO	security.gentoo.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

[179770](#) Debian Security Update for libsndfile (DLA 3058-1)

[500313](#) Alpine Linux Security Update for libsndfile

504081 Alpine Linux Security Update for libsndfile
671077 EulerOS Security Update for libsndfile (EulerOS-SA-2019-2513)
710270 Gentoo Linux libsndfile Multiple Vulnerabilities (GLSA 201811-23)
900330 Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3791)
902837 Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3841)

© [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](#)