



CVE-2017-7742

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

Summary

CVE	CVE-2017-7742
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-12 18:59:00 UTC
Updated	2017-07-11 01:33:00 UTC
Description	In libsndfile before 1.0.28, an error in the "flac_buffer_copy()" function (flac.c) can be exploited to cause a segmentation vio

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libsndfile Project	Libsndfile	All	All	All	All

References

Reference	Source	Link
libsndfile: Multiple vulnerabilities (GLSA 201707-04) — Gentoo security	GENTOO	security.gentoo.org
libsndfile: invalid memory READ and invalid memory WRITE in flac_buffer_copy (flac.c) agostino's blog	MISC	blogs.gentoo.org
src/flac.c: Improve error handling · erikd/libsndfile@60b2343 · 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

[500311](#) Alpine Linux Security Update for libsndfile

[504079](#) Alpine Linux Security Update for libsndfile

[671077](#) EulerOS Security Update for libsndfile (EulerOS-SA-2019-2513)

© [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](#)