



CVE-2017-6892

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

Summary

CVE	CVE-2017-6892
State	PUBLIC
Assigner	PSIRT-CNA@flexerasoftware.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-12 16:29:00 UTC
Updated	2020-10-29 19:15:00 UTC
Description	In libsndfile version 1.0.28, an error in the "aiff_read_chanmap()" function (aiff.c) can be exploited to cause an out-of-bound

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	1.0.28	All	All	All
Application	Libsndfile Project	Libsndfile	1.0.28	All	All	All

References

Reference	Source	Link	Tags
End of Support for the Secunia Community Site - Community	MISC	secuniaresearch.flexerasoftware.com	Third Party
USN-4013-1: libsndfile vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com	
[SECURITY] [DLA 2418-1] libsndfile security update	MLIST	lists.debian.org	
libsndfile: Multiple vulnerabilities (GLSA 201811-23) — Gentoo security	GENTOO	security.gentoo.org	
Computer Security Research - Secunia	MISC	secuniaresearch.flexerasoftware.com	Third Party
src/aiff.c: Fix a buffer read overflow · libsndfile/libsndfile@f833c53 · GitHub	CONFIRM	github.com	Issue Track
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[710270](#) Gentoo Linux libsndfile Multiple Vulnerabilities (GLSA 201811-23)

[900348](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3848)

[902952](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3805)

© [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](#)