



CVE-2019-3832

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

Summary

CVE	CVE-2019-3832
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2023-03-01 18:02:00 UTC
Description	It was discovered the fix for CVE-2018-19758 (libsndfile) was not complete and still allows a read beyond the limits of a buffer.

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
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
wav_write_header: don't read past the array end by epozuelo · Pull Request #460 · erikd/libsndfile · GitHub	CONFIRM
USN-4013-1: libsndfile vulnerabilities Ubuntu security notices	UBUNTU
1677216 – (CVE-2019-3832) CVE-2019-3832 libsndfile: incomplete fix for CVE-2018-19758 still allow to read beyond buffer limits	CONFIRM
[SECURITY] [DLA 2418-1] libsndfile security update	MLIST
Incomplete fix for CVE-2018-19758 · Issue #456 · erikd/libsndfile · GitHub	CONFIRM
libsndfile: Multiple vulnerabilities (GLSA 202007-65) — Gentoo security	GENTOO
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[296078](#) Oracle Solaris 11.4 Support Repository Update (SRU) 16.4.0 Missing (CPUOCT2019)

[500316](#) Alpine Linux Security Update for libsndfile

[504083](#) Alpine Linux Security Update for libsndfile

[690448](#) Free Berkeley Software Distribution (FreeBSD) Security Update for libsndfile (086c96cd-d0cb-11ea-b922-5404a68ad561)

[900459](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3853)

[903271](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3802)

© [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](#)