



CVE-2017-8365

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

Summary

CVE	CVE-2017-8365
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-30 19:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	The i2les_array function in pcm.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer over-read & ...)

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	Tags
libsndfile: global buffer overflow in i2les_array (pcm.c) agostino's blog	MISC	blogs.gentoo.org	Patch, Third Party Advisory, VDB
[SECURITY] [DLA 1618-1] libsndfile security update	MLIST	lists.debian.org	Mailing List, Third Party Advisory
libsndfile: Multiple vulnerabilities (GLSA 201811-23) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500312](#) Alpine Linux Security Update for libsndfile

[504080](#) 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)

[900428](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3845)

[903230](#) Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3803)

© [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](#)