



CVE-2018-13139

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

Summary

CVE	CVE-2018-13139
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-07-04 14:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	A stack-based buffer overflow in psf_memset in common.c in libsndfile 1.0.28 allows remote attackers to cause a denial of s

Risk And Classification

Problem Types: CWE-787

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
USN-4013-1: libsndfile vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.
[SECURITY] [DLA 1618-1] libsndfile security update	MLIST	lists.debian
libsndfile: Multiple vulnerabilities (GLSA 201811-23) — Gentoo security	GENTOO	security.ger
stack-buffer-overflow in psf_memset in libsndfile-master/src/common.c:1229 · Issue #397 · erikd/libsndfile · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

377266 Alibaba Cloud Linux Security Update for libsndfile (ALINUX2-SA-2020:0061)
500314 Alpine Linux Security Update for libsndfile
504082 Alpine Linux Security Update for libsndfile
710270 Gentoo Linux libsndfile Multiple Vulnerabilities (GLSA 201811-23)
750920 SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2021:2615-1)
750972 SUSE Enterprise Linux Security Update for libsndfile (SUSE-SU-2021:2764-1)
750978 OpenSUSE Security Update for libsndfile (openSUSE-SU-2021:2764-1)
751023 OpenSUSE Security Update for libsndfile (openSUSE-SU-2021:1166-1)
900349 Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3852)
902992 Common Base Linux Mariner (CBL-Mariner) Security Update for libsndfile (3794)
940403 AlmaLinux Security Update for libsndfile (ALSA-2020:1636)
960840 Rocky Linux Security Update for libsndfile (RLSA-2020:1636)

© [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](#)