



CVE-2017-7697

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

Summary

CVE	CVE-2017-7697
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-11 23:59:00 UTC
Updated	2022-04-18 18:12:00 UTC
Description	In libsamplerate before 0.1.9, a buffer over-read occurs in the calc_output_single function in src_sinc.c via a crafted audio fi

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	9.0	All	All	All
Application	Libsamplerate Project	Libsamplerate	All	All	All	All

References

Reference	Source	Link	Ta
[SECURITY] [DLA 2845-1] libsamplerate security update	MLIST	lists.debian.org	
libsamplerate 'src_sinc.c' Local Buffer Overflow Vulnerability	BID	www.securityfocus.com	Th
global buffer overflow in calc_output_single (src_sinc.c) · Issue #11 · erikd/libsamplerate · GitHub	CONFIRM	github.com	Iss
CVE Program record	CVE.ORG	www.cve.org	car
NVD vulnerability detail	NVD	nvd.nist.gov	car

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

178938 Debian Security Update for libsamplerate (DLA 2845-1)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)