



CVE-2014-9496

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

Summary

CVE	CVE-2014-9496
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-16 16:59:00 UTC
Updated	2020-11-20 17:34:00 UTC
Description	The sd2_parse_rsrc_fork function in sd2.c in libsndfile allows attackers to have unspecified impact via vectors related to a (

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Libsndfile Project	Libsndfile	All	All	All	All
Application	Libsndfile Project	Libsndfile	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Solaris	11.2	All	All	All

Operating System	Oracle	Solaris	11.2	All	All	All
References						
Reference	Source	Link	Tags			
Mageia Advisory: MGASA-2015-0015 - Updated libsndfile packages fix CVE-2014-9496	CONFIRM	advisories.mageia.org	Third Party			
libsndfile: Multiple vulnerabilities (GLSA 201612-03) — Gentoo security	GENTOO	security.gentoo.org	Third Party			
libsndfile 'src/sd2.c' Multiple Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	Third Party			
Oracle Bulletin Board Update - January 2015	CONFIRM	www.oracle.com	Third Party			
src/sd2.c : Fix two potential buffer read overflows. · dbe14f0 · erikd/libsndfile · GitHub	CONFIRM	github.com	Patch, Thi			
Bugtraq: [SECURITY] [DSA 4430-1] wpa security update	BUGTRAQ	seclists.org	Mailing Lis			
Support / Security / Advisories // MDVSA-2015:024 Mandriva	MANDRIVA	www.mandriva.com	Third Party			
sd2.c: 2 buffer overruns · Issue #93 · erikd/libsndfile · GitHub	CONFIRM	github.com	Exploit, Th			
USN-2832-1: libsndfile vulnerabilities Ubuntu	UBUNTU	www.ubuntu.com	Third Party			
openSUSE-SU-2015:0041-1: moderate: Security update for libsndfile	SUSE	lists.opensuse.org	Mailing Lis			
Security Advisory SA62320 - SUSE update for libsndfile - Secunia	SECUNIA	secunia.com	Third Party			
oss-security - Re: Re: CVE Request: libsndfile buffer overread	MLIST	www.openwall.com	Mailing Lis			
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)						

© 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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.cve.org/). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report