



# CVE-2017-11358

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-11358
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-07-31 13:29:00 UTC
<b>Updated</b>	2023-02-07 01:15:00 UTC
<b>Description</b>	The read_samples function in hcom.c in Sound eXchange (SoX) 14.4.2 allows remote attackers to cause a denial of service

## Risk And Classification

### Problem Types: CWE-125

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	7.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Sound Exchange Project</a>	<a href="#">Sound Exchange</a>	14.4.2	All	All	All
Application	<a href="#">Sound Exchange Project</a>	<a href="#">Sound Exchange</a>	14.4.2	All	All	All

## References

Reference	Source	Link	Tags
oss-security - Re: sox: patches for old vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
Full Disclosure: Sound eXchange (SoX) multiple vulnerabilities	MISC	<a href="http://seclists.org">seclists.org</a>	Exploit, Mailing List, Third Party Advisory
[SECURITY] [DLA 1197-1] sox security update	MLIST	<a href="http://lists.debian.org">lists.debian.org</a>	Third Party Advisory
oss-security - sox: patches for old vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
SoX: Multiple vulnerabilities (GLSA 201810-02) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	Third Party Advisory
oss-security - Re: sox: patches for old vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	
Sound eXchange (SoX) 14.4.2 - Multiple Vulnerabilities - Linux dos Exploit	EXPLOIT-DB	<a href="http://www.exploit-db.com">www.exploit-db.com</a>	Exploit, Third Party Advisory
oss-security - Re: sox: patches for old vulnerabilities	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	

[SECURITY] [DLA 1705-1] sox security update	MLIST	<a href="https://lists.debian.org">lists.debian.org</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [181553](#) Debian Security Update for sox (DLA 3315-1)
- [501254](#) Alpine Linux Security Update for sox
- [670225](#) EulerOS Security Update for sox (EulerOS-SA-2021-1850)
- [710232](#) Gentoo Linux SoX Multiple Vulnerabilities (GLSA 201810-02)

© [CVE.report](https://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.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)