



# CVE-2015-8917

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

## Summary

<b>CVE</b>	CVE-2015-8917
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2016-09-20 14:15:00 UTC
<b>Updated</b>	2018-01-05 02:30:00 UTC
<b>Description</b>	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash)

## Risk And Classification

**Problem Types:** CWE-476

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	15.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	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
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="#">Libarchive</a>	<a href="#">Libarchive</a>	All	All	All	All

## References

Reference	Source	Link	Tags
oss-security - Re: Many invalid memory access issues in libarchive	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Third Party Advisory

libarchive CVE-2015-8917 Denial of Service Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
malformed cab segfaults bsdtar · Issue #505 · libarchive/libarchive · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	
Oracle Linux Bulletin - July 2016	CONFIRM	<a href="http://www.oracle.com">www.oracle.com</a>	
CVE-2015-8917	CONFIRM	<a href="http://security-tracker.debian.org">security-tracker.debian.org</a>	Third Party Advisory
Red Hat Customer Portal	REDHAT	<a href="http://rhn.redhat.com">rhn.redhat.com</a>	
USN-3033-1: libarchive vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>	Third Party Advisory
libarchive: Multiple vulnerabilities (GLSA 201701-03) — Gentoo security	GENTOO	<a href="http://security.gentoo.org">security.gentoo.org</a>	
Many invalid memory access issues in libarchive   The Fuzzing Project	MISC	<a href="http://blog.fuzzing-project.org">blog.fuzzing-project.org</a>	Third Party Advisory
oss-security - Many invalid memory access issues in libarchive	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Third Party Advisory
Debian -- Security Information -- DSA-3657-1 libarchive	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[710502](#) Gentoo Linux libarchive Multiple Vulnerabilities (GLSA 201701-03)

© [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](#).

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