



CVE-2015-8920

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2015-8920 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-09-20 14:15:00 UTC |
| Updated | 2023-09-12 14:45:00 UTC |
| Description | The _ar_read_header function in archive_read_support_format_ar.c in libarchive before 3.2.0 allows remote attackers to ca |

Risk And Classification

Problem Types: CWE-125

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 | 15.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | 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 | 15.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Application | Libarchive | Libarchive | All | All | All | All |
| Operating System | Novell | Suse Linux Enterprise Desktop | 12.0 | sp1 | All | All |
| Operating System | Novell | Suse Linux Enterprise Desktop | 12.0 | sp1 | All | All |
| Operating System | Novell | Suse Linux Enterprise Server | 12.0 | sp1 | All | All |
| Operating System | Novell | Suse Linux Enterprise Server | 12.0 | sp1 | All | All |
| Application | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | sp1 | All | All |
| Operating System | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | sp1 | All | All |
| Operating System | Novell | Suse Linux Enterprise Software Development Kit | 12.0 | sp1 | All | All |

References

| Reference | Source | Link | T |
|---|---------|--|----|
| oss-security - Re: Many invalid memory access issues in libarchive | MLIST | www.openwall.com | T |
| libarchive Stack Underflow CVE-2015-8920 Remote Code Execution Vulnerability | BID | www.securityfocus.com | |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com | |
| Oracle Linux Bulletin - July 2016 | CONFIRM | www.oracle.com | |
| Malformed ar file causes invalid read / stack underflow · Issue #511 · libarchive/libarchive · GitHub | CONFIRM | github.com | |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com | |
| USN-3033-1: libarchive vulnerabilities Ubuntu | UBUNTU | www.ubuntu.com | T |
| libarchive: Multiple vulnerabilities (GLSA 201701-03) — Gentoo security | GENTOO | security.gentoo.org | |
| Many invalid memory access issues in libarchive The Fuzzing Project | MISC | blog.fuzzing-project.org | T |
| oss-security - Many invalid memory access issues in libarchive | MLIST | www.openwall.com | T |
| Debian -- Security Information -- DSA-3657-1 libarchive | DEBIAN | www.debian.org | |
| [security-announce] SUSE-SU-2016:1909-1: important: Security update for | SUSE | lists.opensuse.org | T |
| CVE Program record | CVE.ORG | www.cve.org | ca |
| NVD vulnerability detail | NVD | nvd.nist.gov | ca |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

© [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