



CVE-2016-4302

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2016-4302 |
| State | PUBLIC |
| Assigner | cert@cert.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2016-09-21 14:25:00 UTC |
| Updated | 2017-11-04 01:29:00 UTC |
| Description | Heap-based buffer overflow in the parse_codes function in archive_read_support_format_rar.c in libarchive before 3.2.1 all |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|------------|-------------------------------|---------|--------|---------|----------|
| Application | Libarchive | Libarchive | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Hpc Node Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

| Reference | Source | Link |
|---|---------|--|
| Cisco Talos Blog: The Poisoned Archives | MISC | blog.talosintel.com |
| TALOS-CAN-154 · Issue #719 · libarchive/libarchive · GitHub | CONFIRM | github.com |
| Bug 1348444 – CVE-2016-4302 libarchive: Heap buffer overflow in the Rar decompression functionality | CONFIRM | bugzilla.redhat.com |
| Oracle Linux Bulletin - July 2016 | CONFIRM | www.oracle.com |
| Red Hat Customer Portal | REDHAT | rhn.redhat.com |
| Libarchive CVE-2016-4302 Local Heap Buffer Overflow Vulnerability | BID | www.securityfocus.com |
| Issue 719: Fix for TALOS-CAN-154 · libarchive/libarchive@05caadc · GitHub | CONFIRM | github.com |
| libarchive: Multiple vulnerabilities (GLSA 201701-03) — Gentoo security | GENTOO | security.gentoo.org |
| Cisco Talos - Talos 2016 0154 | MISC | www.talosintel.com |
| Debian -- Security Information -- DSA-3657-1 libarchive | DEBIAN | www.debian.org |
| Oracle Solaris Bulletin - July 2016 | CONFIRM | www.oracle.com |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

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