



Red Hat Product Errata    RHSA-2026:8865 - Security Advisory

# RHSA-2026:8865 - Security Advisory

Issued: 2026-04-20    Updated: 2026-04-20

[Overview](#)[Updated Packages](#)

## Synopsis

Important: libarchive security update

## Type/Severity

Security Advisory: Important

### Red Hat Lightspeed patch analysis

Identify and remediate systems affected by this advisory.

[View affected systems](#) 

## Topic

An update for libarchive is now available for Red Hat Enterprise Linux 10.0 Extended Update Support.

Red Hat Product Security has rated this update as having a security impact of Important. A Common Vulnerability Scoring System (CVSS) base score, which gives a detailed severity rating, is available for each vulnerability from the CVE link(s) in the References section.

## Description

The libarchive programming library can create and read several different streaming archive formats, including GNU tar, cpio, and ISO 9660 CD-ROM images. Libarchive is used notably in the bsdtar utility, scripting language bindings such as python-libarchive, and several popular desktop file managers.

Security Fix(es):

- libarchive: Infinite Loop Denial of Service in RAR5 Decompression via archive\_read\_data() in libarchive (CVE-2026-4111)
- libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing (CVE-2026-4424)

For more details about the security issue(s), including the impact, a CVSS score, acknowledgments, and other related information, refer to the CVE page(s) listed in the References section.

## Solution



For details on how to apply this update, which includes the changes described in this advisory, refer to:

<https://access.redhat.com/articles/11258> 

## Affected Products


- Red Hat Enterprise Linux for x86\_64 - Extended Update Support 10.0 x86\_64
- Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le
- Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x
- Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le
- Red Hat Enterprise Linux for x86\_64 - 4 years of updates 10.0 x86\_64

## Fixes

- [BZ - 2446453](#)  - CVE-2026-4111 libarchive: Infinite Loop Denial of Service in RAR5 Decompression via archive\_read\_data() in libarchive
- [BZ - 2449006](#)  - CVE-2026-4424 libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing

## CVEs

- [CVE-2026-4111](#) 

- [CVE-2026-4424](#) 

## References

- <https://access.redhat.com/security/updates/classification/#important> 

The Red Hat security contact is [secalert@redhat.com](mailto:secalert@redhat.com). More contact details at <https://access.redhat.com/security/team/contact/>.



The navigation menu features the Red Hat logo on the left and social media icons for LinkedIn, YouTube, Facebook, and X on the right. Below these are four expandable menu items: Quick Links, Help, Site Info, and Related Sites, each with a downward-pointing chevron icon.

 Partial system outage



The footer menu includes a small hat icon and a list of links: About Red Hat, Jobs, Events, Locations, Contact Red Hat, Red Hat Blog, and Inclusion at Red Hat.

[Cool Stuff Store](#)

[Red Hat Summit](#)

---

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie preferences](#)