



Red Hat Product Errata    RHSA-2026:8864 - Security Advisory

# RHSA-2026:8864 - 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 9.2 Update Services for SAP Solutions.

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: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing (CVE-2026-4424)
- libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing (CVE-2026-5121)

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 Server - AUS 9.2 x86\_64
- Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
- Red Hat Enterprise Linux for x86\_64 - Update Services for SAP Solutions 9.2 x86\_64
- Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64
- Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x
- Red Hat Enterprise Linux for x86\_64 - Extended Life Cycle 9.2 x86\_64
- Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64
- Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le
- Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x

## Fixes

- [BZ - 2449006](#)  - CVE-2026-4424 libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing
- [BZ - 2452945](#)  - CVE-2026-5121 libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing

## CVEs

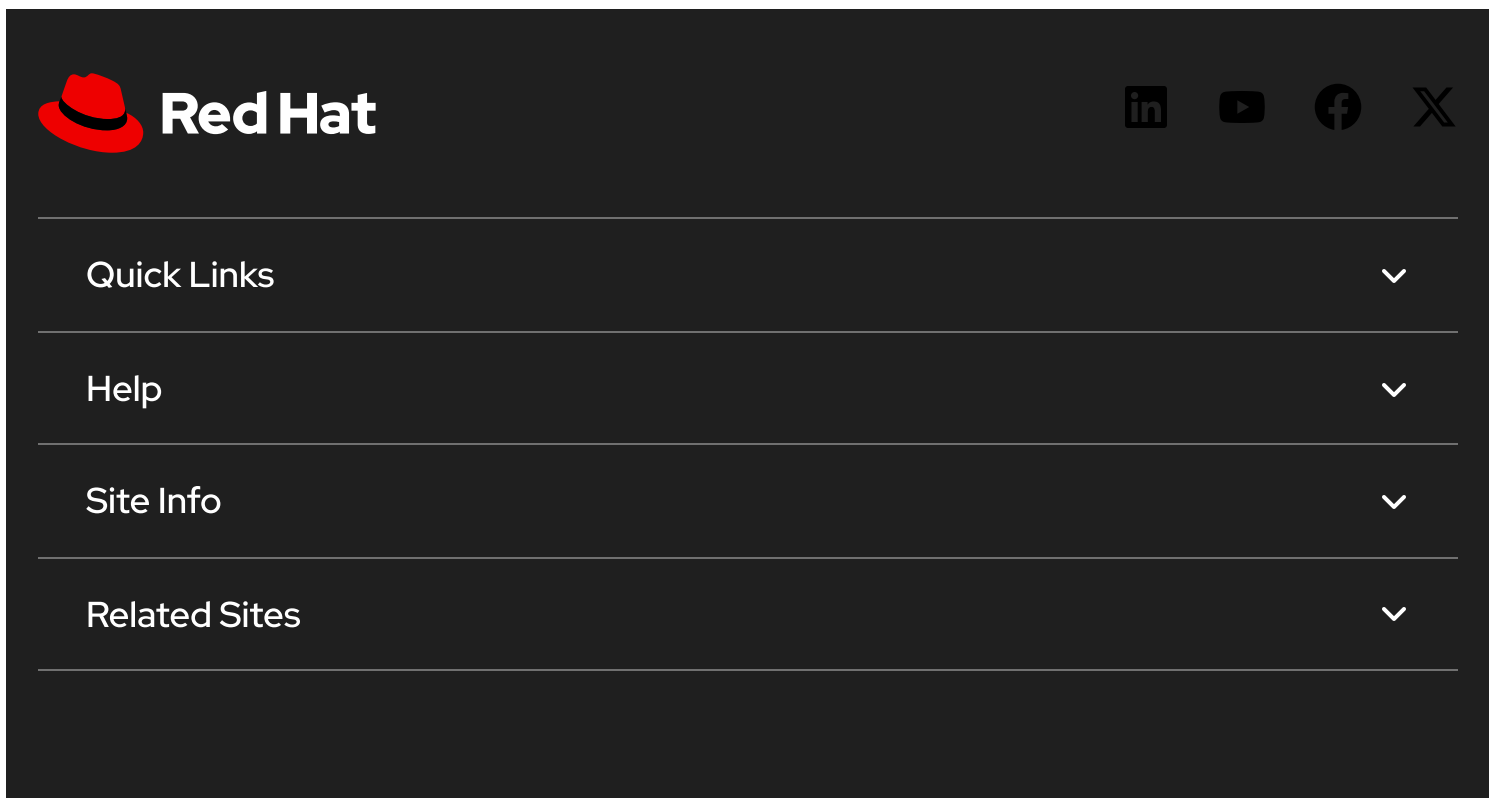
- [CVE-2026-4424](#) 
- [CVE-2026-5121](#) 

## 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 image shows a dark-themed navigation menu for Red Hat. At the top left is the Red Hat logo (a red hat) and the text "Red Hat". To the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below these are four menu items, each with a downward-pointing chevron icon on the right: "Quick Links", "Help", "Site Info", and "Related Sites".

 Partial system outage



The image shows a dark-themed footer for Red Hat. On the left is a small icon of a grey hat. To its right are three links: "About Red Hat", "Jobs", and "Events".

[Locations](#)

[Contact Red Hat](#)

[Red Hat Blog](#)

[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](#)