



Red Hat Product Errata RHSA-2026:6647 - Security Advisory

RHSA-2026:6647 - Security Advisory

Issued: 2026-04-06 Updated: 2026-04-06

[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: Infinite Loop Denial of Service in RAR5 Decompression via archive_read_data() in libarchive (CVE-2026-4111)

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 - 2446453](#)  - CVE-2026-4111 libarchive: Infinite Loop Denial of Service in RAR5 Decompression via archive_read_data() in libarchive

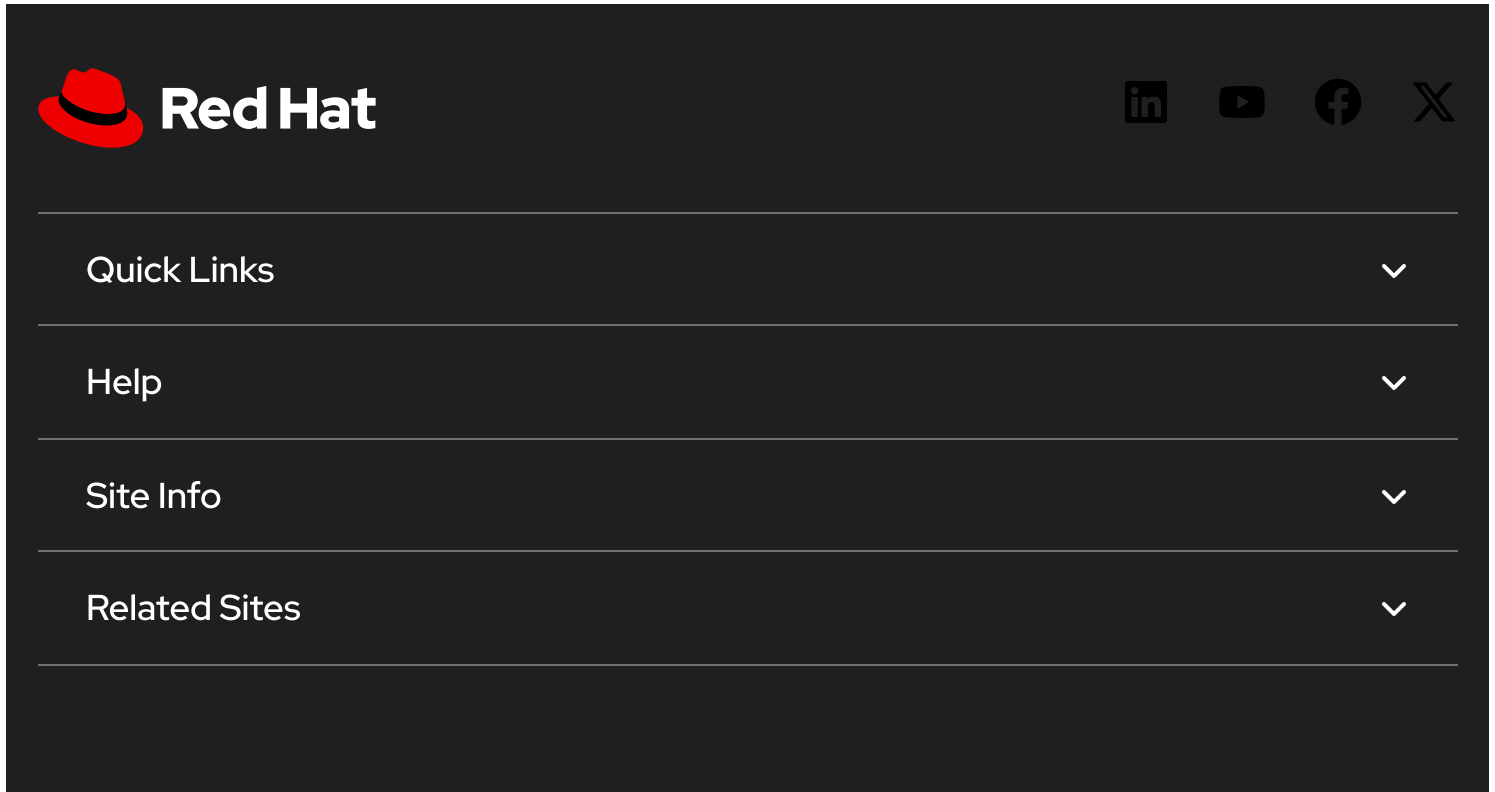
CVEs

- [CVE-2026-4111](#) 


References

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

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



The image shows a dark-themed navigation bar for the Red Hat website. On the left is the Red Hat logo, consisting of a red fedora hat icon and the text "Red Hat". On the right are social media icons for LinkedIn, YouTube, Facebook, and X. Below the logo and icons is a vertical list of navigation items: "Quick Links", "Help", "Site Info", and "Related Sites". Each item has a white downward-pointing chevron icon to its right, indicating a dropdown menu.

 Partial system outage



The image shows a dark-themed footer menu. At the top left is a small, light-colored fedora hat icon. Below the icon is a vertical list of links: "About Red Hat", "Jobs", "Events", "Locations", "Contact Red Hat", "Red Hat Blog", "Inclusion at Red Hat", and "Cool Stuff Store".

Red Hat Summit

© 2026 Red Hat

[Privacy statement](#)

[Terms of use](#)

[All policies and guidelines](#)

[Digital accessibility](#)

[Cookie Preferences and Do Not Sell or Share My Personal Information](#)