RHSA-2026:8517 - Security Advisory

Issued: 2026-04-16 Updated: 2026-04-16

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 7 Extended Lifecycle 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: 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 - Extended Life Cycle Support 7 x86_64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64
- Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le

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. More contact details at https://access.redhat.com/security/team/contact/.

Red Hat

Quick Links

Help

Site Info

Related Sites

Loading

About Red Hat
Jobs
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 and Opt-Out Rights