Bug 2449006 (CVE-2026-4424) - CVE-2026-4424 libarchive: libarchive: Information disclosure via heap out-of-bounds read in RAR archive processing

Keywords: Security

Status: NEW

Alias: CVE-2026-4424

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: high

Severity: high

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 2449007 2449008 2449009

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-19 12:25 UTC by OSIDB Bzimport

Modified: 2026-04-16 16:43 UTC (History)

CC List: 0 users

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2026:8492	0	None	None	None	2026-04-16 14:47:34 UTC
Red Hat Product Errata	RHSA-2026:8510	0	None	None	None	2026-04-16 16:09:58 UTC
Red Hat Product Errata	RHSA-2026:8517	0	None	None	None	2026-04-16 16:40:24 UTC

Red Hat Product Errata	RHSA-2026:8521	0	None	None	None	2026-04-16 16:43:51 UTC

OSIDB Bzimport 2026-03-19 12:25:44 UTC Description

A Heap Out-of-Bounds Read vulnerability exists in the RAR archive processing logic of the libarchive library. The issue arises from improper validation of the LZSS sliding window size after transitions between compression methods (PPMd and LZSS). Due to a mismatch between the allocated buffer size and the expected dictionary size, the copy_from_lzss_window() function performs out-of-bounds memory reads. This allows a specially crafted RAR archive to leak heap memory through the archive_read_data() API before integrity checks (CRC) are enforced. The vulnerability can be exploited remotely without authentication or user interaction in systems that automatically process archives, leading to disclosure of sensitive information.

errata-xmlrpc 2026-04-16 14:47:33 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2026:8492 https://access.redhat.com/errata/RHSA-2026:8492

errata-xmlrpc 2026-04-16 16:09:56 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:8510 https://access.redhat.com/errata/RHSA-2026:8510

errata-xmlrpc 2026-04-16 16:40:23 UTC Comment 4

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 7 Extended Lifecycle Support

Via RHSA-2026:8517 https://access.redhat.com/errata/RHSA-

2026:8517

errata-xmlrpc 2026-04-16 16:43:50 UTC Comment 5

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8.2 Advanced Update Support

Via RHSA-2026:8521 https://access.redhat.com/errata/RHSA-2026:8521

Note

You need to log in before you can comment on or make changes to this bug.