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

Keywords: Security

Status: NEW

Alias: CVE-2026-4111

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: 2448050 2448051 ~~2448049~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-03-11 11:27 UTC by OSIDB Bzimport

Modified: 2026-04-29 08:53 UTC (History)

CC List: 1 user (show)

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	RHBA-2026:5253	0	None	None	None	2026-03-23 02:28:50 UTC
Red Hat Product Errata	RHBA-2026:5379	0	None	None	None	2026-03-23 11:25:35 UTC
Red Hat Product Errata	RHBA-2026:5507	0	None	None	None	2026-03-23 23:28:38 UTC

Red Hat Product Errata	RHBA-2026:5510	0	None	None	None	2026-03-23 22:52:37 UTC
Red Hat Product Errata	RHBA-2026:5564	0	None	None	None	2026-03-24 09:55:04 UTC
Red Hat Product Errata	RHSA-2026:10081	0	None	None	None	2026-04-29 08:53:43 UTC
Red Hat Product Errata	RHSA-2026:5063	0	None	None	None	2026-03-19 08:08:33 UTC
Red Hat Product Errata	RHSA-2026:5080	0	None	None	None	2026-03-19 11:39:52 UTC
Red Hat Product Errata	RHSA-2026:6481	0	None	None	None	2026-04-02 16:17:33 UTC
Red Hat Product Errata	RHSA-2026:6647	0	None	None	None	2026-04-06 09:20:17 UTC
Red Hat Product Errata	RHSA-2026:7093	0	None	None	None	2026-04-08 14:24:39 UTC
Red Hat Product Errata	RHSA-2026:7105	0	None	None	None	2026-04-08 16:36:17 UTC
Red Hat Product Errata	RHSA-2026:7106	0	None	None	None	2026-04-08 16:41:26 UTC
Red Hat Product Errata	RHSA-2026:7239	0	None	None	None	2026-04-16 10:24:12 UTC
Red Hat Product Errata	RHSA-2026:8423	0	None	None	None	2026-04-22 08:27:48 UTC
Red Hat Product Errata	RHSA-2026:8865	0	None	None	None	2026-04-20 02:49:48 UTC

OSIDB Bzimport 2026-03-11 11:27:56 UTC Description

An Infinite Loop Denial-of-Service vulnerability exists in the RAR5 decompression implementation of libarchive. The flaw occurs in the uncompress_file() routine within archive_read_support_format_rar5.c due to a logical deadlock between the filter activation threshold and the half-window output limiter. When a specially crafted RAR5 archive is processed through archive_read_data(), the decompressor enters a state where neither the filter activation condition nor the output window progress condition can be satisfied. As a result, the loop continues indefinitely while consuming 100% CPU. Because the archive passes all CRC and checksum validation, the issue can be triggered using a valid-looking archive without authentication or user interaction. This allows attackers to exhaust worker threads or processing pipelines in applications that automatically extract or scan archives.

errata-xmlrpc 2026-03-19 08:08:32 UTC Comment 2

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 10

Via RHSA-2026:5063 https://access.redhat.com/errata/RHSA-2026:5063

errata-xmlrpc 2026-03-19 11:39:51 UTC Comment 3

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9

Via RHSA-2026:5080 https://access.redhat.com/errata/RHSA-2026:5080

errata-xmlrpc 2026-04-02 16:17:31 UTC Comment 4

This issue has been addressed in the following products:

  Service Interconnect 1 for RHEL 9

Via RHSA-2026:6481 https://access.redhat.com/errata/RHSA-2026:6481

errata-xmlrpc 2026-04-06 09:20:16 UTC Comment 5

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.2 Update Services for SAP Solutions

Via RHSA-2026:6647 https://access.redhat.com/errata/RHSA-2026:6647

errata-xmlrpc 2026-04-08 14:24:38 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2026:7093 https://access.redhat.com/errata/RHSA-2026:7093

errata-xmlrpc 2026-04-08 16:36:16 UTC Comment 7

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.6 Extended Update Support

Via RHSA-2026:7105 https://access.redhat.com/errata/RHSA-2026:7105

errata-xmlrpc 2026-04-08 16:41:25 UTC Comment 8

This issue has been addressed in the following products:

  Red Hat Enterprise Linux 9.4 Extended Update Support

Via RHSA-2026:7106 https://access.redhat.com/errata/RHSA-2026:7106

errata-xmlrpc 2026-04-16 10:24:10 UTC Comment 9

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.13

Via RHSA-2026:7239 https://access.redhat.com/errata/RHSA-

2026:7239

errata-xmlrpc 2026-04-20 02:49:48 UTC Comment 10

This issue has been addressed in the following products:

Red Hat Enterprise Linux 10.0 Extended Update Support

Via RHSA-2026:8865 https://access.redhat.com/errata/RHSA-2026:8865

errata-xmlrpc 2026-04-22 08:27:47 UTC Comment 11

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.18

Via RHSA-2026:8423 https://access.redhat.com/errata/RHSA-2026:8423

errata-xmlrpc 2026-04-29 08:53:42 UTC Comment 14

This issue has been addressed in the following products:

Red Hat OpenShift Container Platform 4.19

Via RHSA-2026:10081 https://access.redhat.com/errata/RHSA-2026:10081

Note

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