



## Bug 2452945 (CVE-2026-5121) - CVE-2026-5121 libarchive: libarchive: Arbitrary code execution via integer overflow in ISO9660 image processing

**Keywords:**

**Reported:** 2026-03-30 07:40 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-04-16 16:43 UTC ([History](#))

**Alias:** CVE-2026-5121

**CC List:** 2 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:**


**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

Attachments	( <a href="#">Terms of Use</a> )

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2026:8510</a>	0	None	None	None	2026-04-16 16:10:01 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:8517</a>	0	None	None	None	2026-04-16 16:40:25 UTC
Red Hat Product Errata	<a href="#">RHSA-2026:8521</a>	0	None	None	None	2026-04-16 16:43:56 UTC

OSIDB Bzimport  2026-03-30 07:40:48 UTC[Description](#)

On 32-bit systems, an integer overflow in the zisofs block pointer allocation logic (archive\_read\_support\_format\_iso9660.c, line 1537) wraps the allocation size to zero. malloc(0) returns a ~16-byte buffer, but the code records the un-wrapped size (~4 GB) and proceeds to memcpy() attacker-controlled ISO data into the tiny buffer - a heap buffer overflow WRITE. On 64-bit systems the overflow doesn't wrap and malloc fails safely. Shares root cause with vulnerability #2 (unvalidated pz\_log2\_bs). Requirements to exploit: The target must be a 32-bit system processing a crafted ISO9660 image via libarchive. The attacker needs to deliver the ISO to an application that extracts or reads its contents. Exploitation to RCE would require heap grooming specific to the target allocator/platform.

errata-xmlrpc 2026-04-16 16:09:59 UTC

[Comment 1](#)

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 16:40:24 UTC

[Comment 2](#)

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 16:43:55 UTC

[Comment 3](#)

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.

