# Bug 2455921 (CVE-2026-5745) - CVE-2026-5745 libarchive: A NULL pointer dereference vulnerability exists in the ACL parser of libarchive

**Keywords:** Security

**Status:** NEW

**Alias:** CVE-2026-5745

**Product:** Security Response

**Component:** vulnerability

**Version:** unspecified

**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

**Reported:** 2026-04-07 14:41 UTC by OSIDB Bzimport

**Modified:** 2026-04-07 14:44 UTC (History)

**CC List:** 0 users

**Fixed In Version:**

**Clone Of:**

**Environment:**

**Last Closed:**

**Embargoed:**

| Attachments (Terms of Use) |
| --- |
| |

OSIDB Bzimport 2026-04-07 14:41:09 UTC Description

A flaw was found in libarchive. A NULL pointer dereference vulnerability exists in the ACL parsing logic, specifically within the archive_acl_from_text_nl() function. When processing a malformed ACL string (such as a bare "d" or "default" tag without subsequent fields), the function fails to perform adequate validation before advancing the pointer. An attacker can exploit this by providing a maliciously crafted archive, causing an application utilizing the libarchive API (such as bsdtar) to crash, resulting in a Denial of Service (DoS).

Note

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