Bug 2455340 (CVE-2026-5673) - CVE-2026-5673 libtheora: libtheora: Denial of Service or Information Disclosure via malformed AVI file processing

Keywords: Security

Status: NEW

Alias: CVE-2026-5673

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: 2455342 2455343

Blocks:

TreeView+ depends on / blocked

Reported: 2026-04-06 09:10 UTC by OSIDB Bzimport

Modified: 2026-04-06 09:17 UTC (History)

CC List: 1 user (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-04-06 09:10:45 UTC Description

A heap-based out-of-bounds read flaw was found in libtheora within the avi_parse_input_file() function in avilib.c. The vulnerability occurs when the AVI parser processes a malformed file containing a truncated hdrl sub-chunk. Because the parser lacks sufficient length validation before performing fixed-offset memcpy operations (such as copying the compressor field), it can be triggered to read past the end of the hdrl_data buffer. A local attacker could exploit this by tricking a user into opening a specially crafted AVI file, leading to a denial-of-service (application crash) or

potentially leaking information from the heap.

Note

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