



Bug 2436982 (CVE-2026-0968) - CVE-2026-0968 libssh: libssh: Denial of Service due to malformed SFTP message

Keywords: Security

Reported: 2026-02-04 23:48 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-10 18:48 UTC ([History](#))

Alias: CVE-2026-0968

CC List: 6 users ([show](#))

Product: Security Response

Fixed In Version:

Component: vulnerability

Clone Of:

Environment:

Version: unspecified

Last Closed:

Embargoed:

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On:

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-04 23:48:10 UTC

[Description](#)

A malicious SFTP server can send malformed longname field of the `SSH_FXP_NAME` message (file listing). Due to the missing NULL check, the libssh could read beyond the buffer bounds on heap, causing unexpected behavior or crashes.

Note

You need to [log in](#) before you can comment on or make changes to this bug.

