



Bug 2436979 (CVE-2026-0964) - CVE-2026-0964 libssh: Improper sanitation of paths received from SCP servers

Keywords: Security

Reported: 2026-02-04 23:40 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-10 18:45 UTC ([History](#))

Alias: CVE-2026-0964

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: medium

Severity: medium

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 23:40:15 UTC[Description](#)

A malicious SCP server can send unexpected paths that could make the client application override local files outside of working directory.
This could be misused to create malicious executable or configuration files and make the user execute them under specific consequences.

This is the same issue as in OpenSSH, tracked as [CVE-2019-6111](#).

Note

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

