



Bug 2436980 (CVE-2026-0965) - CVE-2026-0965 libssh: libssh: Denial of Service via improper configuration file handling

Keywords: Security

Reported: 2026-02-04 23:43 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-02-26 01:29 UTC ([History](#))

Alias: CVE-2026-0965

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

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2442910](#) [2442911](#)

Blocks:

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

Attachments ([Terms of Use](#))

OSIDB Bzimport 2026-02-04 23:43:12 UTC

[Description](#)

libssh can try to open any file during configuration parsing, when misconfigured or when local attacker can provide malicious configuration. This applies for all configuration loaded from default location, configuration provided through the ``ssh_config_parse_file()`` and ``ssh_bind_config_parse_file()`` functions as well as configuration files included from them directly or through glob wildcards.

The possibly dangerous files involve block devices, fifo,

named pipe or
huge system files that could cause Denial of Service.

The solution here is allowing to read only regular files and enforcing configuration file size limit of 16MB. Currently, maximum line length of a configuration file is 1K so this will effectively mean configuration files of 16K lines should still keep working.

Note

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

