Bug 2436981 (CVE-2026-0967) - CVE-2026-0967 libssh: libssh: Denial of Service via inefficient regular expression processing

Keywords: Security

Status: NEW

Alias: CVE-2026-0967

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~2442914~~

Blocks:

TreeView+ depends on / blocked

Reported: 2026-02-04 23:44 UTC by OSIDB Bzimport

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

CC List: 6 users (show)

Fixed In Version:

Clone Of:

Environment:

Last Closed:

Embargoed:

Attachments (Terms of Use)

OSIDB Bzimport 2026-02-04 23:44:40 UTC Description

```
The function `match_pattern()` is used to match conditionals
in client
configuration files or known hosts against the hostname the
client is
connecting to.

When the configuration file or known_hosts file is controlled
by the
attacker, connecting to specific hostnames could cause
timeouts and
resource exhaustion due to the ineffective backtracking of
complex
regular expressions.
```

```
The pattern matching was modified to avoid the needless
backtracing.
```

Note

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