



## Bug 2423148 (CVE-2025-14821) - CVE-2025-14821 libssh: libssh: Insecure default configuration leads to local man-in-the-middle attacks on Windows

**Keywords:** Security

**Reported:** 2025-12-17 11:52 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-02-12 11:52 UTC ([History](#))

**Alias:** CVE-2025-14821

**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  2025-12-17 11:52:26 UTC[Description](#)

An insecure default configuration vulnerability exists in libssh on Windows systems where the library automatically loads configuration files from the C:\etc directory. Since this directory can be created and modified by unprivileged local users, an attacker can inject malicious SSH configuration or known-hosts entries. This enables local man-in-the-middle attacks, security downgrades of SSH connections, and manipulation of trusted host information. Exploitation requires only low privileges and no user interaction, posing a significant risk to the confidentiality, integrity, and availability of SSH communications that rely on libssh.

---

**Note**

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

