CVE-2025-14821

VEX

Public on February 10, 2026
Last modified: April 7, 2026 at 4:17:32 PM UTC

LOW

Low severity
What does this mean?

7.8

CVSS v3 Score Breakdown

Jump to section

Description | Statement | Mitigation | Additional information | Affected Packages | CVSS Score Details | Weakness (CWE) | Acknowledgements | FAQ

Description

A flaw was found in libssh. This vulnerability allows local man-in-the-middle attacks, security downgrades of SSH (Secure Shell) connections, and manipulation of trusted host information, posing a significant risk to the confidentiality, integrity, and availability of SSH communications via an insecure default configuration on Windows systems where the library automatically loads configuration files from the C:\etc directory, which can be created and modified by unprivileged local users.

Statement

This vulnerability is rated Low for Red Hat products. The flaw in libssh is specific to its insecure default configuration on Windows systems, where it loads configuration from the C:\etc directo ry. Red Hat's Linux-based products do not utilize this configuration path, and therefore are not

affected by this vulnerability.

Mitigation

Mitigation for this issue is either not available or the currently available options do not meet the Red Hat Product Security criteria comprising ease of use and deployment, applicability to widespread installation base, or stability.

Additional information

- Bugzilla 2423148: libssh: libssh: Insecure default configuration leads to local man-in-the-middle attacks on Windows
- CWE-427: Uncontrolled Search Path Element

External references

- https://www.cve.org/CVERecord?id=CVE-2025-14821
- https://nvd.nist.gov/vuln/detail/CVE-2025-14821
- https://www.libssh.org/2026/02/10/libssh-0-12-0-and-0-11-4-security-releases/

Affected Packages and Issued Red Hat Security Errata

Unless explicitly stated as not affected, all previous versions of packages in any minor update stream of a product listed here should be assumed vulnerable, although may not have been subject to full analysis.

Search:

Filter by: Products / Services | Components | State

Errata | Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	libssh
State	Not affected
Justification	Vulnerable Code not Present
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 6
Components	libssh2
State	Not affected
Justification	Vulnerable Code not Present
Errata	
Release Date	

Products / Services	Red Hat Enterprise Linux 7
Components	libssh2
State	Not affected
Justification	Vulnerable Code not Present
Errata	

1 of 1

Common Vulnerability Scoring System (CVSS) Score Details

Important note

CVSS scores for open source components depend on vendor-specific factors (e.g. version or build chain). Therefore, Red Hat's score and impact rating can be different from NVD and other vendors. Red Hat remains the authoritative CVE Naming Authority (CNA) source for its products and services (see Red Hat classifications).

The following CVSS metrics and score provided are preliminary and subject to review.

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	7.8	N/A	N/A
Attack Vector	Local	N/A	N/A
Attack Complexity	Low	N/A	N/A
Privileges Required	Low	N/A	N/A
User Interaction	None	N/A	N/A
Scope	Unchanged	N/A	N/A
Confidentiality Impact	High	N/A	N/A
Integrity Impact	High	N/A	N/A
Availability Impact	High	N/A	N/A

CVSS v3 Vector

Red Hat: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Acknowledgements

Red Hat would like to thank Martin Grubhofer for reporting this issue.

Frequently Asked Questions

- **Why is Red Hat's CVSS v3 score or Impact different from other vendors?**
- **My product is listed as "Under investigation" or "Affected", when will Red Hat release a fix for this vulnerability?**
- **What can I do if my product is listed as "Will not fix"?**
- **What can I do if my product is listed as "Fix deferred"?**
- **What is a mitigation?**
- **I have a Red Hat product but it is not in the above list, is it affected?**
- **Why is my security scanner reporting my product as vulnerable to this vulnerability even though my product version is fixed or not affected?**

Not sure what something means? Check out our Security Glossary.

Want to get errata notifications? Sign up here.

For clarification or corrections, please contact Red Hat Product Security.

Last modified: April 7, 2026 at 4:17:32 PM UTC

Red Hat

Quick Links

Help

Site Info

Related Sites

Partial system outage