CVE-2025-5372

VEX

Public on June 24, 2025

Last modified: November 24, 2025 at 9:03:11 PM UTC

MODERATE

Moderate severity

What does this mean?

5

CVSS v3 Score Breakdown

Jump to section

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

Description

A flaw was found in libssh versions built with OpenSSL versions older than 3.0, specifically in the ssh_kdf() function responsible for key derivation. Due to inconsistent interpretation of return values where OpenSSL uses 0 to indicate failure and libssh uses 0 for success—the function may mistakenly return a success status even when key derivation fails. This results in uninitialized cryptographic key buffers being used in subsequent communication, potentially compromising SSH sessions' confidentiality, integrity, and availability.

Statement

The Red Hat Product Security team has assessed the severity of this vulnerability as Moderate due to the combination of limited prerequisites and its impact on confidentiality, integrity, and availability. The vulnerability is only present when libssh is built with OpenSSL versions older than 3.0. Successful exploitation could allow an attacker to initiate cryptographic operations using uninitialized keys, which may compromise secure SSH sessions.

Mitigation

To mitigate this issue, administrators should ensure that libssh is built against OpenSSL version 3.0 or later. This change eliminates the return code mismatch and prevents the erroneous use of uninitialized key material. It is also strongly recommended to apply vendor supplied patches or update to the latest libssh security release as soon as possible.

Additional information

- Bugzilla 2369388: libssh: Incorrect Return Code Handling in ssh_kdf() in libssh
- CWE-682: Incorrect Calculation

External references

- https://www.cve.org/CVERecord?id=CVE-2025-5372
- https://nvd.nist.gov/vuln/detail/CVE-2025-5372

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 8
Components	libssh
State	Fixed
Justification	None
Errata	RHSA-2025:21977
Release Date	November 24, 2025

Products / Services	Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions
Components	libssh
State	Fixed
Justification	None
Errata	RHSA-2025:23024
Release Date	December 10, 2025

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

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).

CVSS v3 Score Breakdown

	Red Hat	NVD	CVE List
CVSS v3 Base Score	5	8.8	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	Low	N/A
Privileges Required	Low	Low	N/A
User Interaction	None	None	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	Low	High	N/A
Integrity Impact	Low	High	N/A
Availability Impact	Low	High	N/A

CVSS v3 Vector

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

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

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?
- My product is listed as "Out of Support Scope". What does this mean?

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: November 24, 2025 at 9:03:11 PM UTC