CVE-2025-5987

VEX

Public on April 26, 2025

Last modified: January 22, 2026 at 12:19:22 AM UTC

MODERATE

Moderate severity

What does this mean?

8.1

CVSS v3 Score Breakdown

Jump to section

Description

A flaw was found in libssh when using the ChaCha20 cipher with the OpenSSL library. If an attacker manages to exhaust the heap space, this error is not detected and may lead to libssh using a partially initialized cipher context. This occurs because the OpenSSL error code returned aliases with the SSH_OK code, resulting in libssh not properly detecting the error returned by the OpenSSL library. This issue can lead to undefined behavior, including compromised data confidentiality and integrity or crashes.

Statement

Red Hat Product Security Team has rated this vulnerability as having a Moderate security impact. This is due to the high complexity in exploiting this flaw. For a successful attack to take place an attacker needs to manage to exhaust the heap space to for the OpenSSL library to return the error code which wrongly match the SSH_OK return code.

Additional information

- Bugzilla 2376219: libssh: Invalid return code for chacha20 poly1305 with OpenSSL backend
- CWE-393: Return of Wrong Status Code

External references

- https://www.cve.org/CVERecord?id=CVE-2025-5987
- https://nvd.nist.gov/vuln/detail/CVE-2025-5987

Affected Packages and Issued Red Hat Security Errata

Search:

Filter by: Products / Services Components State Errata Clear all

Products / Services	Red Hat Enterprise Linux 10
Components	libssh
State	Fixed

Justification	None
Errata	RHSA-2025:23484
Release Date	December 17, 2025

Products / Services	Red Hat Enterprise Linux 10.0 Extended Update Support
Components	libssh
State	Fixed
Justification	None
Errata	RHSA-2026:0427
Release Date	January 12, 2026

Products / Services	Red Hat Enterprise Linux 9

1-10 of 16

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.

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
CVSS v3 Base Score	8.1	8.1
Attack Vector	Network	Network
Attack Complexity	High	High
Privileges Required	None	None
User Interaction	None	None
Scope	Unchanged	Unchanged
Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High

CVSS v3 Vector

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

NVD: CVSS:3.1/AV:N/AC:H/PR:N/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: January 22, 2026 at 12:19:22 AM UTC

Quick Links

Help

Site Info

Related Sites

All systems operational

About Red Hat
Jobs
Events
Locations
Contact Red Hat
Red Hat Blog
Inclusion at Red Hat
Cool Stuff Store
Red Hat Summit

Privacy statement
Terms of use
All policies and guidelines
Digital accessibility
Cookie Preferences and Opt-Out Rights