



Bug 2369388 (CVE-2025-5372) - CVE-2025-5372 libssh: Incorrect Return Code Handling in ssh_kdf() in libssh

Keywords: Security ✕

Reported: 2025-05-30 11:36 UTC by OSIDB Bzimport

Status: NEW

Modified: 2026-04-06 15:01 UTC ([History](#))

Alias: CVE-2025-5372

CC List: 7 users ([show](#))

Deadline: 2025-06-24

Fixed In Version:

Product: Security Response

Clone Of:

Component: vulnerability ☰ +

Environment:

Last Closed:

Embargoed:

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: Product Security DevOps Team

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: [2376282](#) [2376277](#) [2376278](#)
[2376279](#) [2376280](#) [2376281](#)
[2455370](#)

Blocks:


TreeView+ [depends on](#) / [blocked](#)

Attachments [\(Terms of Use\)](#)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHBA-2025:21997	0	None	None	None	2025-11-24 20:24:03 UTC
Red Hat Product Errata	RHBA-2025:21998	0	None	None	None	2025-11-24 20:34:07 UTC

Red Hat Product Errata	RHBA-2025:22081	0	None	None	None	2025-11-25 16:06:04 UTC
Red Hat Product Errata	RHBA-2025:22756	0	None	None	None	2025-12-04 12:55:16 UTC
Red Hat Product Errata	RHBA-2025:22932	0	None	None	None	2025-12-09 15:35:22 UTC
Red Hat Product Errata	RHBA-2025:22933	0	None	None	None	2025-12-09 16:05:47 UTC
Red Hat Product Errata	RHSA-2025:21977	0	None	None	None	2025-11-24 16:54:13 UTC
Red Hat Product Errata	RHSA-2025:23024	0	None	None	None	2025-12-10 10:17:48 UTC

OSIDB Bzimport  2025-05-30 11:36:30 UTC[Description](#)

Incorrect Success Return vulnerability in the ssh_kdf() function of libssh when built with OpenSSL versions prior to 3.0. This issue arises because libssh interprets OpenSSL's return value 0 (indicating failure) as SSH_OK (indicating success). As a result, on failure, the function may return success without initializing the output key buffers. This can lead to the use of uninitialized cryptographic keys, affecting the encryption and decryption of SSH traffic. The vulnerability allows an attacker to exploit improper key handling, potentially resulting in data leakage, integrity issues, or denial of service during SSH communication.

errata-xmlrpc 2025-11-24 16:54:12 UTC

[Comment 1](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 8

Via [RHSA-2025:21977](#) <https://access.redhat.com/errata/RHSA-2025:21977>

errata-xmlrpc 2025-12-10 10:17:46 UTC

[Comment 5](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 9.0 Update Services for SAP Solutions

Via RHSA-2025:23024 <https://access.redhat.com/errata/RHSA-2025:23024>

Note

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

