CVE

VEX

Public o

Last mo

Description

A flaw was found in libssh in which a malicious SFTP (SSH File Transfer Protocol) server can exploit this by sending a malformed 'longname' field within an `SSH_FXP_NAME` message during a file listing operation. This missing null check can lead to reading beyond allocated memory on the heap. This can cause unexpected behavior or lead to a denial of service (DoS) due to application crashes.

Statement

The vulnerability in libssh has been rated as Low by Red Hat Product Security.

This issue affects the libssh client when processing responses from an SFTP server. Succe ssful exploitation requires a user to initiate a connection to a malicious or compromised SF TP server and perform specific operations, such as listing directory contents. As a result, e xploitation is not possible without user interaction.

Additionally, the vulnerability depends on specially crafted protocol responses from a mali cious server, increasing the attack complexity and reducing the likelihood of successful ex ploitation in typical deployments.

The impact of this flaw is limited to a client-side denial-of-service condition, such as an ap plication crash. There is no evidence that this issue can be leveraged to execute arbitrary c ode, access sensitive information, or modify data.

Due to the requirement for user interaction, higher attack complexity, and limited impact on availability only, Red Hat considers this vulnerability to have a lower risk.

Additional information

- Bugzilla 2436982: libssh: libssh: Denial of Service due to malformed SFTP message
- CWE-476: NULL Pointer Dereference

External references

- https://www.cve.org/CVERecord?id=CVE-2026-0968
- https://nvd.nist.gov/vuln/detail/CVE-2026-0968
- 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	Affected
Justification	None
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	3.1	3.1	N/A
Attack Vector	Network	Network	N/A
Attack Complexity	High	High	N/A
Privileges Required	None	None	N/A
User Interaction	Required	Required	N/A
Scope	Unchanged	Unchanged	N/A
Confidentiality Impact	None	None	N/A
Integrity Impact	None	None	N/A
Availability Impact	Low	Low	N/A

CVSS v3 Vector

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

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

Acknowledgements

Red Hat would like to thank Jakub Jelen (libssh) and nevv (CTyun Red-Shield Security Lab) 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 13, 2026 at 8:39:14 PM UTC