

[curl](#) / [Docs](#) / [curl CVEs](#) / **libssh key passphrase bypass without agent set****CVE-2025-15224**

Awarded 505 USD

**Related:**[Audits](#)[Changelog](#)[curl CVEs](#)[JSON metadata](#)[Original report](#)[Vulnerability Disclosure](#)[Vulnerabilities Table](#)

# libssh key passphrase bypass without agent set

Project curl Security Advisory, January 7 2026 - [Permalink](#)

## VULNERABILITY

When doing SSH-based transfers using either SCP or SFTP, and asked to do public key authentication, curl would wrongly still ask and authenticate using a locally running SSH agent.

## INFO

This flaw only exists when libcurl is built to use the libssh backend, not the libssh2 based one. This problem happened because libssh has a somewhat surprising API choice where they fall back to agent authentication.

It should be noted that the authentication still only succeeds if the local SSH agent actually has the correct passphrase.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-15224 to this issue.

CWE-287: Improper Authentication

Severity: Low

# AFFECTED VERSIONS

- Affected versions: curl 7.58.0 to and including 8.17.0
- Not affected versions: curl < 7.58.0 and >= 8.18.0
- Introduced-in:  
<https://github.com/curl/curl/commit/c92d2e14cfb0db662f958effd2ac86f99>

libcurl is used by many applications, but not always advertised as such!

This bug is not considered a *C mistake*. It is not likely to have been avoided had we not been using C.

This flaw **also** affects the curl command line tool.

# SOLUTION

Starting in curl 8.18.0, this mistake is fixed.

- Fixed-in:  
<https://github.com/curl/curl/commit/16d5f2a5660c61cc27bd5f1c7f512391d1c92>

# RECOMMENDATIONS

A - Upgrade curl to version 8.18.0

B - Build curl with the libssh2 backend

C - Avoid using SFTP or SCP

# TIMELINE

This issue was reported to the curl project on December 28, 2025. We contacted [distros@openwall](mailto:distros@openwall) on December 30, 2025.

curl 8.18.0 was released on January 7 2026 around 07:00 UTC, coordinated with the publication of this advisory.

The curl security team is not aware of any active exploits using this vulnerability.

# CREDITS

- Reported-by: Harry Sintonen
- Patched-by: Harry Sintonen

Thanks a lot!