# CVE-2025-15079

Awarded 505 USD

**Related:**
Audits
Changelog
curl CVEs
JSON metadata
Original report
Vulnerability Disclosure
Vulnerabilities Table

# libssh global known_hosts override

Project curl Security Advisory, January 7 2026 - Permalink

## VULNERABILITY

When doing SSH-based transfers using either SCP or SFTP, and setting the known_hosts file, libcurl could still mistakenly accept connecting to hosts *not present* in the specified file if they were added as recognized in the libssh *global* known_hosts file.

## 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 a built-in *global* known_hosts file if the host was not found in the specified one. The global file that was used as a fallback gets its set path at build time.

The fix now makes libcurl set *both* known_hosts files to the same path.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-15079 to this issue.

CWE-297: Improper Validation of Certificate with Host Mismatch

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/adca486c125d9a6d9565b9607a19dce803

# 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 24, 2025. We contacted 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: Daniel Stenberg

Thanks a lot!