CVE-2025-14017

Awarded 2540 USD

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

broken TLS options for threaded LDAPS

Project curl Security Advisory, January 7 2026 Permalink

VULNERABILITY

When doing multi-threaded LDAPS transfers (LDAP over TLS) with libcurl, changing TLS options in one thread would inadvertently change them globally and therefore possibly also affect other concurrently setup transfers.

Disabling certificate verification for a specific transfer could unintentionally disable the feature for other threads as well.

INFO

curl contains support for several different LDAP backends. This flaw only exists when libcurl was built to use the "legacy" non-Windows LDAP support (the `lib/ldap.c` source code). Notably, builds using OpenLDAP are not affected.

It does not apply to users of WinLDAP (the flavor of LDAP provided in Windows) since that API does not offer those TLS related options.

This is only a potential problem when doing LDAP transfers concurrently in more than one thread. The global state was used for the connection setup (only), so this vulnerability is highly timing sensitive.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-14017 to this issue.

CWE-567: Unsynchronized Access to Shared Data in a Multi-threaded Context

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 7.17.0 to and including 8.17.0
- Not affected versions: curl < 7.17.0 and >= 8.18.0
- Introduced-in: https://github.com/curl/curl/commit/ccba0d10b6baf5c73ca

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 **does not** affect the curl command line tool.

SOLUTION

Starting in curl 8.18.0, this mistake is fixed.

- Fixed-in: https://github.com/curl/curl/commit/39d1976b7f709a516e324333

RECOMMENDATIONS

A - Upgrade curl to version 8.18.0

B - Build curl with OpenLDAP

C - Avoid using LDAP

TIMELINE

This issue was reported to the curl project on December 1, 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: Stanislav Fort (Aisle Research)
- Patched-by: Daniel Stenberg

Thanks a lot!