CVE-2025-14819

Awarded 505 USD

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

OpenSSL partial chain store policy bypass

Project curl Security Advisory, January 7 2026 - Permalink

VULNERABILITY

When doing TLS related transfers with reused easy or multi handles and altering the `CURLSSLOPT_NO_PARTIALCHAIN` option, libcurl could accidentally reuse a CA store cached in memory for which the partial chain option was reversed. Contrary to the user's wishes and expectations. This could make libcurl find and accept a trust chain that it otherwise would not.

INFO

As a performance enhancement, in libcurl's OpenSSL related backend code, it holds the loaded CA store cached in memory. This cache is held in memory up to 24 hours by default until refreshed.

The libcurl option `CURLOPT_SSL_OPTIONS` has a bit called `CURLSSLOPT_NO_PARTIALCHAIN` which if set makes libcurl not set the OpenSSL *store flag* called `X509_V_FLAG_PARTIAL_CHAIN`.

curl contains support for several different TLS backends. This flaw only exists when libcurl uses OpenSSL (or one of the many OpenSSL forks) in runtime.

This only affects TLS related transfers and only if `CURLOPT_CA_CACHE_TIMEOUT` is not disabled (set to zero).

libcurl still verifies the certificate and returns error if it cannot, even with this flaw. It just might accept a partial trust chain that it otherwise would not.

Applications *rarely* toggle this option individually for different transfers.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-14819 to this issue.

CWE-295: Improper Certificate Validation

Severity: Low

AFFECTED VERSIONS

- Affected versions: curl 7.87.0 to and including 8.17.0
- Not affected versions: curl < 7.87.0 and >= 8.18.0
- Introduced-in: https://github.com/curl/curl/commit/3c16697ebd796f799227b

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/cd046f6c93b39d673a58c1864

RECOMMENDATIONS

A - Upgrade curl to version 8.18.0

B - Avoid using `CURLSSLOPT_NO_PARTIALCHAIN`

C - Switch off CA caching with `CURLOPT_CA_CACHE_TIMEOUT`

TIMELINE

This issue was reported to the curl project on December 16, 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: Stanislav Fort (Aisle Research)
- Patched-by: Daniel Stenberg

Thanks a lot!