CVE-2025-13034

Awarded 2540 USD

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

No QUIC certificate pinning with GnuTLS

Project curl Security Advisory, January 7 2026 - Permalink

VULNERABILITY

When using `CURLOPT_PINNEDPUBLICKEY` option with libcurl or `--pinnedpubkey` with the curl tool, curl should check the public key of the server certificate to verify the peer.

This check was skipped in a certain condition that would then make curl allow the connection without performing the proper check, thus not noticing a possible impostor. To skip this check, the connection had to be done with QUIC with ngtcp2 built to use GnuTLS and the user had to explicitly disable the standard certificate verification.

INFO

curl contains support for several different QUIC and TLS backends. Other QUIC backends or the ngtcp2 backend built with another TLS library are not affected by this flaw.

If instead connecting to a server over HTTP/1 or HTTP/2, the pinning check works fine and does properly detect impostors.

This issue is similar to CVE-2025-5025 but for a different TLS library.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-13034 to this issue.

CWE-295: Improper Certificate Validation

Severity: Medium

AFFECTED VERSIONS

- Affected versions: curl 8.8.0 to and including 8.17.0
- Not affected versions: curl < 8.8.0 and >= 8.18.0
- Introduced-in: https://github.com/curl/curl/commit/3210101088dfa3d6a125

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/3d91ca8cdb3b434226e743946

RECOMMENDATIONS

A - Upgrade curl to version 8.18.0

B - Build curl with another TLS library

C - Avoid using HTTP/3

TIMELINE

This issue was reported to the curl project on November 9, 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!