CVE-2025-14524

Awarded 505 USD

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

bearer token leak on cross-protocol redirect

Project curl Security Advisory, January 7 2026 - Permalink

VULNERABILITY

When an OAuth2 bearer token is used for an HTTP(S) transfer, and that transfer performs a cross-protocol redirect to a second URL that uses an IMAP, LDAP, POP3 or SMTP scheme, curl might wrongly pass on the bearer token to the new target host.

INFO

By default, curl only allows redirects to HTTP(S) and FTP(S), but can be asked to allow redirects to all protocols curl supports. This vulnerability only triggers for users who use OAuth2 bearer and who actively enable redirects to one of the four protocols mentioned above and one of those schemes is used in the HTTP redirect. A highly unusual combination.

The redirect-to URL needs to have the username component set (but not the password) to trigger this flaw.

This token leak also happens if the redirect is done to the same hostname, just a different protocol (and port).

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-14524 to this issue.

CWE-522: Insufficiently Protected Credentials

Severity: Low

AFFECTED VERSIONS

- Affected versions: curl 7.33.0 to and including 8.17.0
- Not affected versions: curl < 7.33.0 and >= 8.18.0
- Introduced-in: https://github.com/curl/curl/commit/06c1bea72faabb6fad4b7ef8

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/1a822275d333dc6da6043497160fd

RECOMMENDATIONS

A - Upgrade curl to version 8.18.0

B - Avoid allowing cross-protocol redirects

C - Avoid using OAuth2 bearer tokens

TIMELINE

This issue was reported to the curl project on December 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: anonymous237 on hackerone
- Patched-by: Daniel Stenberg

Thanks a lot!