CVE-2025-9086

Awarded 505 USD

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

Out of bounds read for cookie path

Project curl Security Advisory, September 10 2025 - Permalink

VULNERABILITY

1. A cookie is set using the `secure` keyword for `https://target`
2. curl is redirected to or otherwise made to speak with `http://target` (same hostname, but using clear text HTTP) using the same cookie set
3. The same cookie name is set - but with just a slash as path (`path="/"`). Since this site is not secure, the cookie *should* just be ignored.
4. A bug in the path comparison logic makes curl read outside a heap buffer boundary

The bug either causes a crash or it potentially makes the comparison come to the wrong conclusion and lets the clear-text site override the contents of the secure cookie, contrary to expectations and depending on the memory contents immediately following the single-byte allocation that holds the path.

The presumed and correct behavior would be to plainly ignore the second set of the cookie since it was already set as secure on a secure host so overriding it on an insecure host should not be okay.

INFO

The attacker needs to be in control of the `http://` site that uses the same name as the `https://` version, or otherwise possess MITM capability, which probably makes this problem the lesser one.

The attacker has no way to control or guess what is in the heap memory following the path buffer that is being read out of bounds, making it a fragile operation.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2025-9086 to this issue.

CWE-125: Out-of-bounds Read

Severity: Low

AFFECTED VERSIONS

- Affected versions: curl 8.13.0 to and including 8.15.0
- Not affected versions: curl < 8.13.0 and >= 8.16.0
- Introduced-in: https://github.com/curl/curl/commit/1aea05a6c2699e80c7593

libcurl is used by many applications, but not always advertised as such!

This bug is considered a *C mistake*. It is likely to have been avoided had we not been using C.

This flaw does not affect the curl command line tool. While the curl tool can be tricked to override the cookie in the same way, that does not make it a vulnerability for the tool.

SOLUTION

Starting in curl 8.16.0, this mistake is fixed.

- Fixed-in: https://github.com/curl/curl/commit/c6ae07c6a541e0e96d0040afb6

RECOMMENDATIONS

A - Upgrade curl to version 8.16.0

B - Apply the patch to your local version

C - Avoid using `http://` for cookies

TIMELINE

This issue was reported to the curl project on August 11, 2025. We contacted distros@openwall on September 5, 2025.

curl 8.16.0 was released on September 10 2025 around 06:00 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: Google Big Sleep
- Patched-by: Daniel Stenberg

Thanks a lot!