CVE-2016-8623

Use after free via shared cookies

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

Project curl Security Advisory, November 2 2016
Permalink

VULNERABILITY

libcurl explicitly allows users to share cookies between multiple easy handles that are concurrently employed by different threads.

When cookies to be sent to a server are collected, the matching function collects all cookies to send and the cookie lock is released immediately afterwards. That function however only returns a list with *references* back to the original strings for name, value, path and so on. Therefore, if another thread quickly takes the lock and frees one of the original cookie structs together with its strings, a use after free can occur and lead to information disclosure. Another thread can also replace the contents of the cookies from separate HTTP responses or API calls.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8623 to this issue.

CWE-416: Use After Free

Severity: High

AFFECTED VERSIONS

This flaw exists in the following curl versions:

- Affected versions: curl 7.10.7 to and including 7.50.3
- Not affected versions: curl < 7.10.7 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/41ae97e710f728495a1d6a

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

SOLUTION

In version 7.51.0, the function returning the cookies make deep copies.

- Fixed-in: https://github.com/curl/curl/commit/c5be3d7267c725dbd093ff3a

RECOMMENDATIONS

We suggest you take one of the following actions immediately, in order of preference:

A - Upgrade curl and libcurl to version 7.51.0

B - Apply the patch to your version and rebuild

C - Do not share cookies between threads

TIMELINE

It was first reported to the curl project on September 23 by Cure53.

We contacted distros@openwall on October 19.

curl 7.51.0 was released on November 2 2016, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Cure53
- Patched-by: Daniel Stenberg

his vulnerability was found during a Secure Open Source audit performed by Cure53.