CVE-2016-8615

cookie injection for other servers

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

Project curl Security Advisory, November 2, 2016 - Permalink

VULNERABILITY

If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.

The issue pertains to the function that loads cookies into memory, which reads the specified file into a fixed-size buffer in a line-by-line manner using the `fgets()` function. If an invocation of `fgets()` cannot read the whole line into the destination buffer due to it being too small, it truncates the output. This way, a long cookie (name + value) sent by a malicious server would be stored in the file and subsequently that cookie could be read partially and crafted correctly, it could be treated as a different cookie for another server.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8615 to this issue.

CWE-187: Partial Comparison

Severity: High

AFFECTED VERSIONS

This flaw exists in the following curl versions.

- Affected versions: curl 4.9 to and including 7.50.3
- Not affected versions: curl < 4.9 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/ae1912cb0d494b48d514d9

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

SOLUTION

In version 7.51.0, the cookie read function ignores too long lines.

- Fixed-in: https://github.com/curl/curl/commit/cff89bc088b7884098ea0c5378b

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 use the `CURLOPT_COOKIEFILE` (or `-b`) option.

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

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