CVE-2016-8624

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

invalid URL parsing with '#'

Project curl Security Advisory, November 2, 2016 - Permalink

VULNERABILITY

curl does not parse the authority component of the URL correctly when the host name part ends with a hash (`#`) character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use a URL parser that follows the RFC to check for allowed domains before using curl to request them.

Passing in `http://example.com#@evil.com/x.txt` would wrongly make curl send a request to evil.com while your browser would connect to example.com given the same URL.

The problem exists for most protocol schemes.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8624 to this issue.

CWE-172: Encoding Error

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following curl versions.

- Affected versions: curl 6.0 to and including 7.50.3
- Not affected versions: curl < 6.0 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/ae1912cb0d494b48d5

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

SOLUTION

In version 7.51.0, the parser function is fixed.

- Fixed-in: https://github.com/curl/curl/commit/3bb273db7e40ebc284cff45f3ce3

As a side-effect of this fix, using the `#` character as part of the user or password fields in the URL is no longer supported. According to RFC 3986 section 2.3 it is not allowed. See issue #1216

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 - Strip out the parts of the URLs containing '#' before passing them to curl

TIMELINE

It was first reported to the curl project on October 10.

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: Fernando Muñoz
- Patched-by: Daniel Stenberg

Thanks a lot!