CVE-2016-8621

curl_getdate read out of bounds

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

Project curl Security Advisory, November 2, 2016 - Permalink

VULNERABILITY

The `curl_getdate` converts a given date string into a numerical timestamp and it supports a range of different formats and possibilities to express a date and time. The underlying date parsing function is also used internally when parsing for example HTTP cookies (possibly received from remote servers) and it can be used when doing conditional HTTP requests.

The date parser function uses the libc `sscanf()` function at two places, with the parsing strings `%02d:%02d` and `%02d:%02d:%02d`. The intent being that it would parse either a string with HH:MM (two digits colon two digits) or `HH:MM:SS` (two digits colon two digits colon two digits). If instead the piece of time that was sent in had the final digit cut off, thus ending with a single-digit, the date parser code would advance its read pointer one byte too much and end up reading out of bounds.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-8621 to this issue.

CWE-126: Buffer Over-read

Severity: Medium

AFFECTED VERSIONS

This flaw exists in the following curl versions.

- Affected versions: curl 7.12.2 to and including 7.50.3
- Not affected versions: curl < 7.12.2 and curl >= 7.51.0
- Introduced-in: https://github.com/curl/curl/commit/f6433211ae9afb30ec461e

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/96a80b5a262fb6dd2ddcea7987

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

TIMELINE

It was first reported to the curl project on October 3.

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: Luật Nguyễn
- Patched-by: Daniel Stenberg

Thanks a lot!