CVE-2018-16842

Awarded 100 USD

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

warning message out-of-buffer read

Project curl Security Advisory, October 31st 2018 - Permalink

VULNERABILITY

curl contains a heap out of buffer read vulnerability.

The command line tool has a generic function for displaying warning and informational messages to stderr for various situations. For example if an unknown command line argument is used, or passed to it in a "config" file.

This display function formats the output to wrap at 80 columns. The wrap logic is however flawed, so if a single word in the message is itself longer than 80 bytes the buffer arithmetic calculates the remainder wrong and ends up reading behind the end of the buffer. This could lead to information disclosure or crash.

This vulnerability could lead to a security issue if used in this or similar situations:

1. a server somewhere uses the curl command line to run something
2. if it fails, it shows stderr to the user
3. the server takes user input for parts of its command line input
4. user provides something overly long that triggers this crash
5. the stderr output may now contain user memory contents that was not meant to be available

INFO

This flaw exists in the command line tool only, not in libcurl.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-16842 to this issue.

CWE-125: Out-of-bounds Read

Severity: Low

AFFECTED VERSIONS

- Affected versions: curl 7.14.1 to and including 7.61.1
- Not affected versions: curl < 7.14.1 and >= 7.62.0
- Introduced-in: https://github.com/curl/curl/commit/d9ca9154d1

curl is used by many applications, but not always advertised as such.

SOLUTION

- Fixed-in: https://github.com/curl/curl/commit/d530e92f59ae9bb2d47066

RECOMMENDATIONS

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

A - Upgrade curl to version 7.62.0

B - Apply the patch to your version and rebuild

TIMELINE

It was reported to the curl project on October 27, 2018. We contacted distros@openwall on October 28.

curl 7.62.0 was released on October 31 2018, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Brian Carpenter (Geeknik Labs)
- Patched-by: Daniel Stenberg

Thanks a lot!