CVE-2017-8817

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

FTP wildcard out of bounds read

Project curl Security Advisory, November 29th 2017 - Permalink

VULNERABILITY

libcurl contains a read out of bounds flaw in the FTP wildcard function.

libcurl's FTP wildcard matching feature, which is enabled with the `CURLOPT_WILDCARDMATCH` option can use a built-in wildcard function or a user provided one. The built-in wildcard function has a flaw that makes it not detect the end of the pattern string if it ends with an open bracket (`[`) but instead it continues reading the heap beyond the end of the URL buffer that holds the wildcard.

For applications that use HTTP(S) URLs, allow libcurl to handle redirects and have FTP wildcards enabled, this flaw can be triggered by malicious servers that can redirect clients to a URL using such a wildcard pattern.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2017-8817 to this issue.

CWE-126: Buffer Over-read

Severity: Medium

AFFECTED VERSIONS

- Affected versions: libcurl 7.21.0 to and including 7.56.1
- Not affected versions: libcurl < 7.21.0 and >= 7.57.0
- Introduced-in: https://github.com/curl/curl/commit/0825cd80a62c

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

SOLUTION

In libcurl version 7.57.0, there is a better check for the end of the string. Additionally, the wildcard feature is turned off if the URL passed to libcurl is not using FTP(S), so a redirect to an FTP URL cannot trigger wildcard functionality.

- Fixed-in: https://github.com/curl/curl/commit/0b664ba968437715819b

RECOMMENDATIONS

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

A - Upgrade curl to version 7.57.0

B - Apply the patch to your version and rebuild

C - Do not use `CURLOPT_WILDCARDMATCH` without carefully verifying the patterns used.

TIMELINE

It was reported to the curl project on November 10, 2017. We contacted distros@openwall on November 21.

curl 7.57.10 was released on November 29 2017, coordinated with the publication of this advisory.

CREDITS

- Reported-by: OSS-Fuzz
- Help-by: Max Dymond
- Patched-by: Daniel Stenberg

Thanks a lot!