CVE-2020-8285

FTP wildcard stack overflow

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

Project curl Security Advisory, December 9th 2020 - Permalink

VULNERABILITY

libcurl offers a wildcard matching functionality, which allows a callback (set with `CURLOPT_CHUNK_BGN_FUNCTION`) to return information back to libcurl on how to handle a specific entry in a directory when libcurl iterates over a list of all available entries.

When this callback returns `CURL_CHUNK_BGN_FUNC_SKIP`, to tell libcurl to not deal with that file, the internal function in libcurl then calls itself recursively to handle the next directory entry.

If there is a sufficient amount of file entries and if the callback returns "skip" enough number of times, libcurl runs out of stack space. The exact amount does of course vary with platforms, compilers and other environmental factors.

The content of the remote directory is not kept on the stack, so it seems hard for the attacker to control exactly what data that overwrites the stack - however it remains a Denial-Of-Service vector as a malicious user who controls a server that a libcurl-using application works with under these premises can trigger a crash.

(There is also a few other ways the function can be made to call itself and trigger this problem.)

INFO

This issue was unfortunately reported publicly in the curl GitHub issue tracker as issue 6255.

This functionality is not used by the curl tool so it is not affected. Further: it is not a widely used feature.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2020-8285 to this issue.

CWE-674: Uncontrolled Recursion

Severity: Medium

AFFECTED VERSIONS

- Affected versions: libcurl 7.21.0 to and including 7.73.0
- Not affected versions: libcurl < 7.21.0 and libcurl >= 7.74.0
- Introduced-in: https://github.com/curl/curl/commit/0825cd80a

Also note that libcurl is used by many applications, and not always advertised as such.

SOLUTION

The internal function is rewritten to instead and more appropriately use an ordinary loop instead of the recursive approach. This way, the stack use remains the same no matter how many files that are skipped.

- Fixed-in: https://github.com/curl/curl/commit/69a358f2186e04

RECOMMENDATIONS

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

A - Upgrade libcurl to version 7.74.0

B - Disable FTP wildcard use (`CURLOPT_WILDCARDMATCH`)

C - Make sure your `CURLOPT_CHUNK_BGN_FUNCTION` callback does not do multiple skips.

TIMELINE

This issue was first reported to the curl project on November 27, 2020.

This advisory was posted on December 9th 2020.

CREDITS

- Reported-by: xnynx on github
- Patched-by: Daniel Stenberg

Thanks a lot!