CVE-2019-5481

Awarded 200 USD

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

FTP-KRB double free

Project curl Security Advisory, September 11 2019
Permalink

VULNERABILITY

libcurl can be told to use kerberos over FTP to a server, as set with the `CURLOPT_KRBLEVEL` option.

During such kerberos FTP data transfer, the server sends data to curl in blocks with the 32-bit size of each block first and then that amount of data immediately following.

A malicious or just broken server can claim to send a large block and if by doing that it makes curl's subsequent call to `realloc()` to fail, curl would then misbehave in the exit path and double free the memory.

In practical terms, an up to 4 GB memory area may well be fine to allocate on a modern 64-bit system but on 32-bit systems it fails.

Kerberos FTP is a rarely used protocol with curl. Also, Kerberos authentication is usually only attempted and used with servers that the client has a previous association with.

INFO

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2019-5481 to this issue.

CWE-415: Double Free

Severity: Medium

AFFECTED VERSIONS

- Affected versions: libcurl >= 7.52.0 to and including 7.65.3
- Not affected versions: libcurl < 7.52.0 and libcurl >= 7.66.0
- Introduced-in: https://github.com/curl/curl/commit/0649433da53c7165f839e2

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

SOLUTION

- Fixed-in: https://github.com/curl/curl/commit/9069838b30fb3b48af0123e3

RECOMMENDATIONS

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

A - Upgrade curl to version 7.66.0

B - Apply the patch to your version and rebuild

C - do not use `CURLOPT_KRBLEVEL`

TIMELINE

The issue was reported to the curl project on September 3, 2019. The fix was done, verified and communicated with the reporter on September 3, 2019.

We contacted distros@openwall on September 5.

This advisory was posted on September 11th 2019.

CREDITS

- Reported-by: Thomas Vegas
- Patched-by: Daniel Stenberg

Thanks a lot!