Alpine Linux - Bug #9992

Bug # 9990 (Closed): curl: Multiple vulnerabilities (CVE-2018-16890, CVE-2019-3822, CVE-2019-3823)

[3.8] curl: Multiple vulnerabilities (CVE-2018-16890, CVE-2019-3822, CVE-2019-3823)

02/20/2019 10:39 AM - Alicha CH

Status:	Closed	**Start date:**	02/20/2019
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Description

CVE-2018-16890: NTLM type-2 out-of-bounds buffer read

The function handling incoming NTLM type-2 messages (lib/vauth/ntlm.c:ntlm_decode_type2_target) does not validate incoming data correctly and is subject to an integer overflow vulnerability.
Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.

Affected versions:

libcurl 7.36.0 to and including 7.63.0

Not affected versions:

libcurl < 7.36.0 and >= 7.64.0

References:

https://curl.haxx.se/docs/CVE-2018-16890.html

Patch:

https://github.com/curl/curl/commit/b780b30d1377adb10bbe774835f49e9b237fb9bb

CVE-2019-3822: NTLMv2 type-3 header stack buffer overflow

The function creating an outgoing NTLM type-3 header (lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening.
This output data can grow larger than the local buffer if very large "nt response" data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a "large value" needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.

Affected versions:

libcurl 7.36.0 to and including 7.63.0

Not affected versions:

libcurl < 7.36.0 and >= 7.64.0

References:

https://curl.haxx.se/docs/CVE-2019-3822.html

Patch:

https://github.com/curl/curl/commit/86724581b6c

CVE-2019-3823: SMTP end-of-response out-of-bounds read

If the buffer passed to smtp_endofresp() isn't NUL terminated and contains no character ending the parsed number, and len is set to 5,
then the strtol() call reads beyond the allocated buffer. The read contents will not be returned to the caller.

Affected versions:

libcurl 7.34.0 to and including 7.63.0

Not affected versions:

libcurl < 7.34.0

References:

https://curl.haxx.se/docs/CVE-2019-3823.html

Patch:

https://github.com/curl/curl/commit/39df4073e5413fcdbb5a38da0c1ce6f1c0ceb484

Associated revisions

Revision 5ba18f0c - 03/05/2019 08:31 AM - Leonardo Arena

main/curl: security fixes

CVE-2018-16890, CVE-2019-3822, CVE-2019-3823

Fixes #9992

History

#1 - 03/05/2019 08:31 AM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:5ba18f0ca5e2e4f2371cf806a531c993d2b9689b.

#2 - 03/05/2019 11:26 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed