Alpine Linux - Bug #9612

Bug # 9610 (Closed): curl: Multiple vulnerabilities (CVE-2018-16839, CVE-2018-16840, CVE-2018-16842)

[3.8] curl: Multiple vulnerabilities (CVE-2018-16839, CVE-2018-16840, CVE-2018-16842)

11/01/2018 10:54 AM - Alicha CH

Status:	Closed	**Start date:**	11/01/2018
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:**	

Description

CVE-2018-16839: SASL password overflow via integer overflow

The internal function Curl_auth_create_plain_message fails to correctly verify that the passed in lengths
for name and password aren't too long, then calculates a buffer size to allocate.

On systems with a 32 bit size_t, the math to calculate the buffer size triggers an integer overflow when the user name length exceeds 2GB (2^31 bytes).
This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow.

Affected versions:

libcurl 7.33.0 to and including 7.61.1

Not affected versions:

libcurl < 7.33.0 and >= 7.62.0

Reference:

https://curl.haxx.se/docs/CVE-2018-16839.html

Patch:

https://github.com/curl/curl/commit/f3a24d7916b9173c69a3e0ee790102993833d6c5

CVE-2018-16840: use-after-free in handle close

When closing and cleaning up an "easy" handle in the Curl_close() function, the library code first frees a struct (without nulling the pointer) and might
then subsequently erroneously write to a struct field within that already freed struct.

Affected versions:

libcurl 7.59.0 to and including 7.61.1

Not affected versions:

libcurl < 7.59.0 and >= 7.62.0

Reference:

https://curl.haxx.se/docs/CVE-2018-16840.html

Patch:

https://github.com/curl/curl/commit/81d135d67155c5295b1033679c606165d4e28f3f

CVE-2018-16842: warning message out-of-buffer read

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 will end up reading behind the end of the buffer. This could lead to information disclosure or crash.

Reference:

https://curl.haxx.se/docs/CVE-2018-16842.html

Patch:

https://github.com/curl/curl/commit/d530e92f59ae9bb2d47066c3c460b25d2ffeb211

Associated revisions

Revision d84961d2 - 11/06/2018 02:22 PM - Leonardo Arena

main/curl: security fixes

(CVE-2018-16839, CVE-2018-16840, CVE-2018-16842)

Fixes #9612

History

#1 - 11/06/2018 02:23 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:d84961d2c2bf448d72bbe0cbcc3d08d37bb88dab.

#2 - 11/08/2018 08:31 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-16839, CVE-2018-16840, CVE-2018-16842)