



Bug 1622707 (CVE-2018-14618) - CVE-2018-14618 curl: NTLM password overflow via integer overflow

Keywords: ✕ ▼

Status: CLOSED ERRATA

Alias: CVE-2018-14618

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: low

Severity: low

Target Milestone: ---

Assignee: Red Hat Product Security

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: 1623697 1623698

1625563 1625564

1714209

Blocks: 1622708

TreeView+ [depends on](#) / [blocked](#)

Reported: 2018-08-27 19:40 UTC by Pedro Sampaio

Modified: 2021-12-10 17:10 UTC ([History](#))

CC List: 27 users ([show](#))

Fixed In Version: curl 7.61.1

Clone Of:

Environment:

Last Closed: 2019-07-12 13:05:57 UTC

Embargoed:

Attachments	(Terms of Use)
--------------------	--------------------------------

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:36:48 UTC
Red Hat Product Errata	RHSA-2019:1880	0	None	None	None	2019-07-29 15:13:11 UTC

Pedro Sampaio 2018-08-27 19:40:19 UTC

[Description](#)

NTLM password overflow via integer overflow
=====

Project curl Security Advisory, September 5th 2018 -
[Permalink](<https://curl.haxx.se/docs/CVE-2018-XXXX.html>)

VULNERABILITY

libcurl contains a buffer overflow in the NTLM authentication code.

The internal function `Curl_ntlm_core_mk_nt_hash` multiplies the `length` of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap.

The `length` value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit `size_t`, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2³¹ 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.

(This bug is almost identical to [CVE-2017-8816](<https://curl.haxx.se/docs/CVE-2017-8816.html>).

We are not aware of any exploit of this flaw.

INFO

This bug was introduced in commit [be285cde3f](<https://github.com/curl/curl/commit/be285cde3f>), April 2006.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2018-XXXX to this issue.

CWE-131: Incorrect Calculation of Buffer Size

AFFECTED VERSIONS

This is only an issue on 32 bit systems. It also requires the password field to use more than 2GB of memory, which in itself should be rare.

- Affected versions: libcurl 7.15.4 to and including 7.61.0
- Not affected versions: libcurl < 7.15.4 and >= 7.61.1

curl is used by many applications, but not always advertised

as such.

THE SOLUTION

In libcurl version 7.61.1, the integer overflow is avoided.

A [patch for CVE-2018-XXXX](<https://curl.haxx.se/CVE-2018-bf5f.patch>) is available.

RECOMMENDATIONS

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

A - Upgrade curl to version 7.61.1

B - Apply the patch to your version and rebuild

C - Put length restrictions on the password you can pass to libcurl

TIME LINE

It was [publicly reported] (<https://github.com/curl/curl/issues/2756>) to the curl project on July 18, 2018. We contacted distros@openwall on August 27.

curl 7.61.1 was released on September 5 2018, coordinated with the publication of this advisory.

CREDITS

Reported by Zhaoyang Wu. Patch by Daniel Stenberg.

~~Scott Gayou~~ 2018-08-29 22:19:04 UTC

[Comment 3](#)

No dice using a crafted .netrc or inputting large values in the password prompt that pops up if -u is passed in.

Tried triggering this directly via setting a 2GB password through libcurl (res = curl_easy_setopt(curl, CURLOPT_PASSWORD, pass) on a 32-bit system. Unfortunately, curl_easy_setopt for CURLOPT_PASSWORD does a strdup, which naturally fails. Curl then returns out of memory before hitting the target code.

So this flaw may be possible to hit on 32-bit, but I'm unclear how. There needs to be a code path that directly takes user input without copying it. May exist, but I've looked down five or so avenues and haven't found it yet.

The code does show a pretty trivial heap overflow, but getting

there seems mildly difficult.

~~Doran Moppert~~ 2018-09-03 02:03:08 UTC

[Comment 5](#)

Acknowledgments:

Name: the Curl project
Upstream: Zhaoyang Wu

~~Doran Moppert~~ 2018-09-03 02:03:19 UTC

[Comment 6](#)

External References:

<https://curl.haxx.se/docs/CVE-2018-14618.html>

Andrej Nemeec 2018-09-05 08:47:09 UTC

[Comment 7](#)

Public via:

<https://seclists.org/oss-sec/2018/q3/217>

Andrej Nemeec 2018-09-05 08:47:48 UTC

[Comment 8](#)

Created curl tracking bugs for this issue:

Affects: fedora-all [[bug-1625563](#)]

Tomas Hoger 2018-11-11 21:36:54 UTC

[Comment 10](#)

Upstream commit:

<https://github.com/curl/curl/commit/57d299a499155d4b327e341c6024e293b0418243>

errata-xmlrpc 2018-11-13 08:36:36 UTC

[Comment 11](#)

This issue has been addressed in the following products:

Red Hat Software Collections for Red Hat Enterprise Linux 6
Red Hat Software Collections for Red Hat Enterprise Linux 7
Red Hat Software Collections for Red Hat Enterprise Linux
7.4 EUS
Red Hat Software Collections for Red Hat Enterprise Linux
7.5 EUS
Red Hat Software Collections for Red Hat Enterprise Linux
7.6 EUS

Via RHSA-2018:3558 <https://access.redhat.com/errata/RHSA-2018:3558>

Product Security DevOps Team 2019-07-12 13:05:57 UTC

[Comment 14](#)

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

<https://access.redhat.com/security/cve/cve-2018-14618>

errata-xmlrpc 2019-07-29 15:13:09 UTC

[Comment 15](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2019:1880 <https://access.redhat.com/errata/RHSA-2019:1880>

Note

You need to [log in](#) before you can comment on or make changes to this bug.

