Bug 1388377 (CVE-2016-8617) - CVE-2016-8617 curl: Out-of-bounds write via unchecked multiplication

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2016-8617

Product: Security Response

Component: vulnerability

Version: unspecified

Hardware: All

OS: Linux

Priority: medium

Severity: medium

Target Milestone: ---

Assignee: ~~Red Hat Product Security~~

QA Contact:

Docs Contact:

URL:

Whiteboard:

Depends On: ~~1390894~~ ~~1390895~~ ~~1390896~~

Blocks: 1388393

TreeView+ depends on / blocked

Reported: 2016-10-25 08:18 UTC by ~~Andrej Nemec~~

Modified: 2021-02-17 03:08 UTC (History)

CC List: 34 users (show)

Fixed In Version: curl 7.51.0

Clone Of:

Environment:

Last Closed: 2019-06-08 03:00:54 UTC

Embargoed:

Attachments	(Terms of Use)	
Upstream patch (739 bytes, patch) 2016-10-25 08:54 UTC, ~~Andrej Nemec~~	*no flags*	Details | Diff
		View All

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2018:2486	0	None	None	None	2018-08-16 16:07:10 UTC
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:33:03 UTC

~~Andrej Nemec~~ 2016-10-25 08:18:06 UTC Description

```
In libcurl's base64 encode function, the output buffer is
allocated as follows
without any checks on insize:

     malloc( insize * 4 / 3 + 4 )

On systems with 32-bit addresses in userspace (e.g. x86, ARM,
x32), the
multiplication in the expression wraps around if insize is at
least 1GB of
data. If this happens, an undersized output buffer will be
allocated, but the
full result will be written, thus causing the memory behind
the output buffer
to be overwritten.

If a username is set directly via `CURLOPT_USERNAME` (or
curl's `-u, --user`
option), this vulnerability can be triggered. The name has to
be at least
512MB big in a 32bit system.

Systems with 64 bit versions of the `size_t` type are not
affected by this
issue.

External References:

https://curl.haxx.se/docs/adv_20161102C.html
```

~~Andrej Nemec~~ 2016-10-25 08:54:49 UTC Comment 1

Created attachment 1213772 [details]
Upstream patch

~~Adam Mariš~~ 2016-11-02 08:26:32 UTC Comment 2

Created curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1390894~~]

~~Adam Mariš~~ 2016-11-02 08:26:47 UTC Comment 3

Created mingw-curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1390895~~]

Affects: epel-7 [bug 1390896]

errata-xmlrpc 2018-08-16 16:06:56 UTC Comment 6

This issue has been addressed in the following products:

  Red Hat JBoss Core Services

Via RHSA-2018:2486 https://access.redhat.com/errata/RHSA-2018:2486

errata-xmlrpc 2018-11-13 08:32:48 UTC Comment 7

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

Note

You need to log in before you can comment on or make changes to this bug.