Bug 1388388 (CVE-2016-8623) - CVE-2016-8623 curl: Use-after-free via shared cookies

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2016-8623

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: ~~1390894~~ ~~1390895~~ ~~1390896~~

Blocks: 1388393

TreeView+ depends on / blocked

Reported: 2016-10-25 08:36 UTC by ~~Andrej Nemec~~

Modified: 2021-02-17 03:07 UTC (History)

CC List: 34 users (show)

Fixed In Version: curl 7.51.0

Clone Of:

Environment:

Last Closed: 2019-06-08 03:01:05 UTC

Embargoed:

Attachments	(Terms of Use)	
Upstream patch (6.45 KB, patch) 2016-10-25 10:16 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 16:08:08 UTC
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:33:54 UTC

~~Andrej Nemec~~ 2016-10-25 08:36:50 UTC Description

```
libcurl explicitly allows users to share cookies between
multiple easy handles
that are concurrently employed by different threads.

When cookies to be sent to a server are collected, the
matching function
collects all cookies to send and the cookie lock is released
immediately
afterwards. That funcion however only returns a list with
*references* back to
the original strings for name, value, path and so on.
Therefore, if another
thread quickly takes the lock and frees one of the original
cookie structs
together with its strings, a use-after-free can occur and lead
to information
disclosure. Another thread can also replace the contents of
the cookies from
separate HTTP responses or API calls.

External References:

https://curl.haxx.se/docs/adv_20161102I.html
```

~~Andrej Nemec~~ 2016-10-25 10:16:35 UTC Comment 1

```
Created attachment 1213818 [details]
Upstream patch
```

~~Adam Mariš~~ 2016-11-02 08:29:14 UTC Comment 2

```
Created curl tracking bugs for this issue:

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

~~Adam Mariš~~ 2016-11-02 08:29:29 UTC Comment 3

```
Created mingw-curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1390895~~]
Affects: epel-7 [~~bug 1390896~~]
```

~~Stefan Cornelius~~ 2016-11-03 09:42:21 UTC Comment 4

There are some barriers here: an application needs to use libcurl via the "easy API", has to threaded, and on top of that a racy condition has to be triggered, which is probably hard to influence from the outside/malicious servers. I currently don't think that this is a significant problem in a RHEL context.

errata-xmlrpc 2018-08-16 16:07:43 UTC Comment 7

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 08:33:42 UTC Comment 8

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.