Bug 1388386 (CVE-2016-8622) - CVE-2016-8622 curl: URL unescape heap overflow via integer truncation

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2016-8622

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 08:32 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 03:01:03 UTC

Embargoed:

Attachments	(Terms of Use)	
Upstream patch (4.25 KB, patch) 2016-10-25 09:02 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 16:07:57 UTC
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:33:55 UTC

~~Andrej Nemec~~ 2016-10-25 08:32:56 UTC Description

```
The URL percent-encoding decode function in libcurl is called
`curl_easy_unescape`. Internally, even if this function would
be made to
allocate a unscape destination buffer larger than 2GB, it
would return that
new length in a signed 32 bit integer variable, thus the
length would get
either just truncated or both truncated and turned negative.
That could then
lead to libcurl writing outside of its heap based buffer.

This can be triggered by a user on a 64bit system if the user
can send in a
custom (very large) URL to a libcurl using program.

External References:

https://curl.haxx.se/docs/adv_20161102H.html
```

~~Andrej Nemec~~ 2016-10-25 09:02:01 UTC Comment 1

Created attachment 1213778 [details]
Upstream patch

~~Adam Mariš~~ 2016-11-02 08:28:46 UTC Comment 2

Created curl tracking bugs for this issue:

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

~~Adam Mariš~~ 2016-11-02 08:29:00 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 16:07:41 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 08:33:39 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.