



Bug 1388382 (CVE-2016-8620) - CVE-2016-8620 curl: Glob parser write/read out of bounds

Keywords: Security ✕

Reported: 2016-10-25 08:25 UTC by Andrej Nemeec

Status: CLOSED ERRATA

Modified: 2021-10-21 19:52 UTC [\(History\)](#)

Alias: CVE-2016-8620

CC List: 31 users [\(show\)](#)

Product: Security Response

Fixed In Version: curl 7.51.0

Component: vulnerability

Clone Of:

Version: unspecified

Environment:

Hardware: All

Last Closed: 2021-10-21 19:52:26 UTC

OS: Linux

Embargoed:

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](#)

Attachments		(Terms of Use)	
Upstream patch (4.64 KB, patch) 2016-10-25 08:58 UTC, Andrej Nemeec	<i>no flags</i>	Details Diff	
View All			

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:33:23 UTC

Andrej Nemeec	2016-10-25 08:25:56 UTC	Description
-------------------------------	-------------------------	-----------------------------

The curl tool's "globbing" feature allows a user to specify a numerical range through which curl will iterate. It is typically specified as [1-5], specifying the first and the last numbers in the range. Or with [a-z], using letters.

1. The curl code for parsing the second *unsigned* number did not check for a leading minus character, which allowed a user to specify `[1-1]` with no complaints and have the latter `-1` number get turned into the largest unsigned long value the system can handle. This would ultimately cause curl to write outside the dedicated malloced buffer after no less than 100,000 iterations, since it would have room for 5 digits but not 6.

2. When the range is specified with letters, and the ending letter is left out `[L-]`, the code would still advance its read pointer 5 bytes even if the string was just 4 bytes and end up reading outside the given buffer.

External References:

https://curl.haxx.se/docs/adv_20161102F.html

~~Andrej Nemeč~~ 2016-10-25 08:58:37 UTC

[Comment 1](#)

Created [attachment 1213776](#) [details]
Upstream patch

~~Adam Mariš~~ 2016-11-02 08:27:53 UTC

[Comment 2](#)

Created curl tracking bugs for this issue:

Affects: fedora-all [[bug-1390894](#)]

~~Adam Mariš~~ 2016-11-02 08:28:06 UTC

[Comment 3](#)

Created mingw-curl tracking bugs for this issue:

Affects: fedora-all [[bug-1390895](#)]

Affects: epel-7 [[bug-1390896](#)]

errata-xmlrpc 2018-11-13 08:33:13 UTC

[Comment 4](#)

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.

