



## Bug 1388370 (CVE-2016-8615) - CVE-2016-8615 curl: Cookie injection for other servers

**Keywords:** Security

**Status:** CLOSED ERRATA

**Alias:** CVE-2016-8615

**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 08:09 UTC by Andrej Nemeec

**Modified:** 2021-03-11 14:46 UTC ([History](#))

**CC List:** 36 users ([show](#))

**Fixed In Version:** curl 7.51.0

**Clone Of:**

**Environment:**

**Last Closed:** 2019-06-08 03:00:50 UTC

**Embargoed:**

Attachments		(Terms of Use)	
<a href="#">Upstream patch</a> (1.80 KB, patch) 2016-10-25 08:48 UTC, Andrej Nemeec	<i>no flags</i>	<a href="#">Details</a>   <a href="#">Diff</a>	
<a href="#">View All</a>			

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2018:2486</a>	0	None	None	None	2018-08-16 16:07:10 UTC
Red Hat Product Errata	<a href="#">RHSA-2018:3558</a>	0	None	None	None	2018-11-13 08:32:41 UTC

Andrej Nemeč	2016-10-25 08:09:27 UTC	Description
<p>If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.</p> <p>The issue pertains to the function that loads cookies into memory, which reads the specified file into a fixed-size buffer in a line-by-line manner using the <code>fgets()</code> function. If an invocation of <code>fgets()</code> cannot read the whole line into the destination buffer due to it being too small, it truncates the output. This way, a very long cookie (name + value) sent by a malicious server would be stored in the file and subsequently that cookie could be read partially and crafted correctly, it could be treated as a different cookie for another server.</p> <p>External References:</p> <p><a href="https://curl.haxx.se/docs/adv_20161102A.html">https://curl.haxx.se/docs/adv_20161102A.html</a></p>		

Andrej Nemeč	2016-10-25 08:48:09 UTC	Comment 1
<p>Created <a href="#">attachment 1213756 [details]</a> Upstream patch</p>		

Adam Mariš	2016-11-02 08:25:37 UTC	Comment 2
<p>Created curl tracking bugs for this issue:</p> <p>Affects: fedora-all [ <a href="#">bug-1390894</a> ]</p>		

Adam Mariš	2016-11-02 08:25:52 UTC	Comment 3
<p>Created mingw-curl tracking bugs for this issue:</p> <p>Affects: fedora-all [ <a href="#">bug-1390895</a> ] Affects: epel-7 [ <a href="#">bug-1390896</a> ]</p>		

errata-xmlrpc 2018-08-16 16:06:53 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 08:32:24 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.

