



## Bug 1388390 (CVE-2016-8624) - CVE-2016-8624 curl: Invalid URL parsing with '#'

**Keywords:** Security

**Reported:** 2016-10-25 08:39 UTC by Andrej Nemeec

**Status:** CLOSED ERRATA

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

**Alias:** CVE-2016-8624

**CC List:** 34 users (show)

**Product:** Security Response

**Fixed In Version:** curl 7.51.0

**Component:** vulnerability

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

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

**OS:** Linux

**Priority:** medium

**Embargoed:**

**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)                 |  |
|--|-----------------|--------------------------------|--|
| <a href="#">Upstream patch</a> (2.30 KB, patch)<br>2016-10-25 10:17 UTC, Andrej Nemeec | kdudka: review- | <a href="#">Details   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 16:08:00 UTC |
| Red Hat Product Errata | <a href="#">RHSA-2018:3558</a> | 0       | None     | None   | None    | 2018-11-13 08:34:00 UTC |

| Andrej Nemeec  | 2016-10-25 08:39:13 UTC | Description |
|--|-------------------------|-------------|
| <p>curl doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.</p> <p>Passing in <code>`http://example.com#@evil.com/x.txt`</code> would wrongly make curl send a request to evil.com while your browser would connect to example.com given the same URL.</p> <p>The problem exists for most protocol schemes.</p> <p>External References:</p> <p><a href="https://curl.haxx.se/docs/adv_20161102J.html">https://curl.haxx.se/docs/adv_20161102J.html</a></p> |                         |             |

| Andrej Nemeec  | 2016-10-25 10:17:06 UTC | Comment 1 |
|--|-------------------------|-----------|
| <p>Created <a href="#">attachment 1213819</a> [details]<br/>Upstream patch</p> |                         |           |

| Adam Mariš  | 2016-11-02 08:29:42 UTC | Comment 2 |
|---|-------------------------|-----------|
| <p>Created curl tracking bugs for this issue:<br/>Affects: fedora-all [ <a href="#">bug-1390894</a> ]</p> |                         |           |

| Adam Mariš  | 2016-11-02 08:29:57 UTC | Comment 3 |
|---|-------------------------|-----------|
| <p>Created mingw-curl tracking bugs for this issue:<br/>Affects: fedora-all [ <a href="#">bug-1390895</a> ]<br/>Affects: epel-7 [ <a href="#">bug-1390896</a> ]</p> |                         |           |

| Kamil Dudka | 2016-11-04 15:15:47 UTC | Comment 4 |
|-------------|-------------------------|-----------|
|             |                         |           |

Comment on [attachment 1213819 \[details\]](#)  
Upstream patch

The patch seems to cause an unintended change in behavior:

<https://curl.haxx.se/mail/lib-2016-11/0059.html>

Kamil Dudka 2016-11-07 09:36:47 UTC

[Comment 5](#)

Upstream considers the current behavior correct:

<https://curl.haxx.se/mail/lib-2016-11/0084.html>

... and wants to check file:// URLs stricter to provide better diagnostic messages in case the syntax is misused (namely allow to use only "localhost" or an empty string as the <host> part of the URL).

However, we need to make sure to keep the current (though undocumented) behavior of file://FILE\_FROM\_CURRENT\_DIR unchanged while backporting the security fix for RHEL-6 and RHEL-7.

errata-xmlrpc 2018-08-16 16:07:45 UTC

[Comment 8](#)

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 08:33:46 UTC

[Comment 9](#)

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.

