



## Bug 1644124 (CVE-2018-16842) - CVE-2018-16842 curl: Heap-based buffer over-read in the curl tool warning formatting

**Keywords:** Security ✕

**Reported:** 2018-10-30 05:12 UTC by Sam Fowler

**Status:** CLOSED ERRATA

**Modified:** 2021-12-10 18:06 UTC [\(History\)](#)

**Alias:** CVE-2018-16842

**CC List:** 29 users [\(show\)](#)

**Product:** Security Response

**Fixed In Version:** curl 7.62.0

**Component:** vulnerability

**Clone Of:**

**Version:** unspecified

**Environment:**

**Hardware:** All

**Last Closed:** 2019-08-06 13:20:30 UTC

**OS:** Linux

**Embargoed:**

**Priority:** low

**Severity:** low

**Target Milestone:** ---

**Assignee:** Red Hat Product Security

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [1644558](#) [1644559](#) [1644560](#)  
 [1649809](#) [1649810](#)

**Blocks:** [1644126](#)

**TreeView+** [depends on](#) / [blocked](#)

<b>Attachments</b>	<a href="#">(Terms of Use)</a>
--------------------	--------------------------------

### Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	<a href="#">RHSA-2019:2181</a>	0	None	None	None	2019-08-06 12:25:02 UTC

Sam Fowler	2018-10-30 05:12:16 UTC	<a href="#">Description</a>
<p>Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the <code>tool_msgs.c:voutf()</code> function.</p>		

This display function formats the output to wrap at 80 columns. The wrap logic is however flawed, so if a single word in the message is itself longer than 80 bytes the buffer arithmetic calculates the remainder wrong and will end up reading behind the end of the buffer. This could lead to information disclosure or crash.

Sam Fowler 2018-10-30 05:19:04 UTC

[Comment 1](#)

Acknowledgments:

Name: the Curl project  
Upstream: Brian Carpenter (Geeknik Labs)

Sam Fowler 2018-10-31 07:03:54 UTC

[Comment 2](#)

External Reference:

<https://curl.haxx.se/docs/CVE-2018-16842.html>

Upstream Patch:

<https://github.com/curl/curl/commit/d530e92f59ae9bb2d47066c3c460b25d2ffeb211>

Sam Fowler 2018-10-31 07:04:35 UTC

[Comment 3](#)

Created curl tracking bugs for this issue:

Affects: fedora-all [ [bug-1644558](#) ]

Created mingw-curl tracking bugs for this issue:

Affects: epel-7 [ [bug-1644559](#) ]

Tomas Hoger 2018-11-14 13:42:59 UTC

[Comment 5](#)

It should be noted that this issue only affects the curl command line tool, it does not affect the libcurl library. The flaw is in the function that formats curl's warning and notice messages. Messages are wrapped to 80 characters per line and hence long messages are split across multiple lines. Those messages are used to print information about invalid or malformed options specified for the tool, hence they only

contain trusted input in most use case and no trust boundary is crossed when invalid option is specified. There does not seem to be any use of the warning function for printing any data from the remote servers.

The impact of the problem varies depending on the curl version. In the current curl versions, the vulnerable code can be found in the voutf() function, and the function does not enforce any limit on the message length. This is important, as the calculation goes off by one for every output line printed (if the line only contains text that was split in the middle of the word rather than at white space).

In curl versions prior to 7.58.0, the message is first printed into a 256 bytes long stack-based buffer. This limits the number of times a long word can be wrapped to 3, and that also limits the size of the overflow.

<https://github.com/curl/curl/commit/5d0ba70e17bde74d9a9108c38558f6491d2b5c4d>  
<https://github.com/curl/curl/issues/2174>

In curl versions prior to 7.45.0, the vulnerable code can be found in the warnf() functions. In the commit linked below, the code was moved to voutf(), and warnf() was modified to call voutf(). The new function notef() was added as another caller of voutf().

<https://github.com/curl/curl/commit/481e0de00a9003b9c5220b120e3fc302d9b0932d>

This is the version of the code as used in the curl packages in Red Hat Enterprise Linux 7 and 6.

In curl versions prior to 1.16.3, there is a bug in the wrapping code that causes curl to print long words in a way that only one character is printed on each line. This increases the size of the over-read.

<https://github.com/curl/curl/commit/70b1900dd13d16f2e83f571407a614541d5ac9ba>  
<https://sourceforge.net/p/curl/bugs/652/>

This is the version of the code as used in the curl packages in Red Hat Enterprise Linux 5.

errata-xmlrpc 2019-08-06 12:25:01 UTC

[Comment 9](#)

This issue has been addressed in the following products:

Red Hat Enterprise Linux 7

Via RHSA-2019:2181 <https://access.redhat.com/errata/RHSA-2019:2181>

Product Security DevOps Team 2019-08-06 13:20:30 UTC

[Comment 10](#)

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

<https://access.redhat.com/security/cve/cve-2018-16842>

---

Note

You need to [log in](#) before you can comment on or make changes to this bug.

