Bug 1406712 (CVE-2016-9586) - CVE-2016-9586 curl: printf floating point buffer overflow

Keywords: Reopened, Security

Status: CLOSED ERRATA

Alias: CVE-2016-9586

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: ~~1406716~~ ~~1406717~~ ~~1406718~~

Blocks: 1406719

TreeView+ depends on / blocked

Reported: 2016-12-21 10:11 UTC by ~~Andrej Nemec~~

Modified: 2021-10-21 11:58 UTC (History)

CC List: 33 users (show)

Fixed In Version: curl 7.52.0

Clone Of:

Environment:

Last Closed: 2021-10-21 11:58:41 UTC

Embargoed:

Attachments	(Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2018:3558	0	None	None	None	2018-11-13 08:34:20 UTC

~~Andrej Nemec~~ 2016-12-21 10:11:52 UTC Description

```
libcurl's implementation of the printf() functions triggers a
buffer overflow
when doing a large floating point output. The bug occurs when
the conversion
```

outputs more than 255 bytes.

The flaw happens because the floating point conversion is using system
functions without the correct boundary checks.

The functions have been documented as deprecated for a long time and users are
discouraged from using them in "new programs" as they are planned to get
removed at a future point. But as the functions are present and there's
nothing preventing users from using them, we expect there to be a certain
amount of existing users in the wild.

If there are any application that accepts a format string from the outside
without necessary input filtering, it could allow remote attacks.

This flaw does not exist in the command line tool.

We are not aware of any exploit of this flaw.

References:

http://seclists.org/oss-sec/2016/q4/719

External References:

https://curl.haxx.se/docs/adv_20161221A.html

Upstream patch:

https://curl.haxx.se/CVE-2016-9586.patch

~~Andrej Nemec~~ 2016-12-21 10:12:18 UTC Comment 1

Acknowledgments:

Name: the Curl project

~~Andrej Nemec~~ 2016-12-21 10:21:36 UTC Comment 2

Created curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1406716~~]

~~Andrej Nemec~~ 2016-12-21 10:21:54 UTC Comment 3

Created mingw-curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1406717~~]
Affects: epel-7 [~~bug 1406718~~]

~~Doran Moppert~~ 2016-12-22 03:55:27 UTC Comment 4

This flaw is present in the curl_*printf (curlx_*printf) family of functions, which are not used by curl but are exposed from libcurl. I can't find any of these functions being used across Enterprise Linux.

To be exposed, third-party code would need to be using these long-deprecated functions, with a floating-point specifier and user-controlled (floating-point) input. The overflow itself is of a 256-byte stack-allocated buffer, when the decimal expansion of the float exceeds that by up to 70 bytes. Beyond about 16 digits for a double, the decimal expansion is effectively random so the attacker has very little control over precisely what bytes are written. I think the chance of ACE can be discounted here.

Kamil Dudka 2016-12-23 08:48:28 UTC Comment 5

upstream commit:

https://github.com/curl/curl/commit/curl-7_51_0-162-g3ab3c16

errata-xmlrpc 2018-11-13 08:34:08 UTC Comment 6

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.