



Bug 1642203 (CVE-2018-16840) - CVE-2018-16840 curl: Use-after-free when closing "easy" handle in Curl_close()

Keywords:

Status: CLOSED ERRATA

Alias: CVE-2018-16840

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: [1644555](#) [1644556](#) [1644557](#)
 [1652660](#)

Blocks: [1642204](#)

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

Reported: 2018-10-24 01:51 UTC by Sam Fowler

Modified: 2021-12-10 18:02 UTC ([History](#))

CC List: 30 users ([show](#))

Fixed In Version: curl 7.62.0

Clone Of:

Environment:

Last Closed: 2021-10-25 09:51:37 UTC

Embargoed:

Attachments ([Terms of Use](#))

Sam Fowler 2018-10-24 01:51:43 UTC

[Description](#)

Curl versions 7.59.0 to 7.61.1 are vulnerable to heap use-after-free flaw in code related to closing an easy handle.

When closing and cleaning up an "easy" handle in the ``Curl_close()`` function, the library code first frees a struct (without nulling the pointer) and might then subsequently erroneously write to a struct field within that already

freed struct.

Sam Fowler 2018-10-24 01:52:01 UTC

[Comment 1](#)

Acknowledgments:

Name: the Curl project

Upstream: Brian Carpenter (Geeknik Labs)

Sam Fowler 2018-10-31 07:02:05 UTC

[Comment 2](#)

External Reference:

<https://curl.haxx.se/docs/CVE-2018-16840.html>

Upstream Patch:

<https://github.com/curl/curl/commit/81d135d67155c5295b1033679c606165d4e28f3f>

Sam Fowler 2018-10-31 07:02:42 UTC

[Comment 3](#)

Created curl tracking bugs for this issue:

Affects: fedora-all [[bug-1644555](#)]

Created mingw-curl tracking bugs for this issue:

Affects: epel-7 [[bug-1644556](#)]

Note

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

