Bug 1670252 (CVE-2018-16890) - CVE-2018-16890 curl: NTLM type-2 heap out-of-bounds buffer read

Keywords: Security

Status: CLOSED ERRATA

Alias: CVE-2018-16890

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: ~~1672902~~ 1674357 1674358

Blocks: 1670258

TreeView+ depends on / blocked

Reported: 2019-01-29 04:10 UTC by Sam Fowler

Modified: 2021-02-16 22:28 UTC (History)

CC List: 29 users (show)

Fixed In Version: curl 7.64.0

Clone Of:

Environment:

Last Closed: 2019-11-06 00:51:57 UTC

Embargoed:

Attachments (Terms of Use)

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2019:3701	0	None	None	None	2019-11-05 22:06:06 UTC

Sam Fowler 2019-01-29 04:10:28 UTC Description

```
libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to
a heap buffer out-of-bounds read.
```

The function handling incoming NTLM type-2 messages (`lib/vauth/ntlm.c:ntlm_decode_type2_target`) does not validate incoming data correctly and is subject to an integer overflow vulnerability.

Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.

Bug introduced by:

https://github.com/curl/curl/commit/86724581b6c

Sam Fowler 2019-01-29 04:10:30 UTC Comment 1

Acknowledgments:

Name: Daniel Stenberg (the Curl project)
Upstream: Wenxiang Qian (Tencent Blade Team)

Sam Fowler 2019-02-06 07:45:58 UTC Comment 2

External Reference:

https://curl.haxx.se/docs/CVE-2018-16890.html

Upstream Patch:

https://github.com/curl/curl/commit/b780b30d

Sam Fowler 2019-02-06 07:46:07 UTC Comment 3

Created curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1672902~~]

Huzaifa S. Sidhpurwala 2019-02-11 06:42:40 UTC Comment 6

Mitigation:

Turn off NTLM authentication.

~~Eric Christensen~~ 2019-02-18 14:19:21 UTC Comment 7

```
Statement:

The versions of curl package shipped with Red Hat Enterprise
Linux 5, 6, and 7 do not support NTLMv2 type-2 headers, hence
they are not affected by this flaw.
```

errata-xmlrpc 2019-11-05 22:06:05 UTC Comment 10

```
This issue has been addressed in the following products:

  Red Hat Enterprise Linux 8

Via RHSA-2019:3701 https://access.redhat.com/errata/RHSA-
2019:3701
```

Product Security DevOps Team 2019-11-06 00:51:57 UTC Comment 11

```
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-2018-16890
```

Note

You need to log in before you can comment on or make changes to this bug.