# Bug 1388385 (CVE-2016-8621) - CVE-2016-8621 curl: curl_getdate out-of-bounds read

**Keywords:** Security

**Status:** CLOSED ERRATA

**Alias:** CVE-2016-8621

**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:** ~~1390894~~ ~~1390895~~ ~~1390896~~

**Blocks:** 1388393

**TreeView+** depends on / blocked

**Reported:** 2016-10-25 08:29 UTC by ~~Andrej Nemec~~

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

**CC List:** 33 users (show)

**Fixed In Version:** curl 7.51.0

**Clone Of:**

**Environment:**

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

**Embargoed:**

| Attachments | (Terms of Use) | |
|---|---|---|
| **Upstream patch** (3.90 KB, patch)<br>2016-10-25 09:00 UTC, ~~Andrej Nemec~~ | *no flags* | Details \| Diff |
| | | View All |

**Links**

| System | ID | Private | Priority | Status | Summary | Last Updated |
|---|---|---|---|---|---|---|
| Red Hat Product Errata | RHSA-2018:2486 | 0 | None | None | None | 2018-08-16 16:07:34 UTC |
| Red Hat Product Errata | RHSA-2018:3558 | 0 | None | None | None | 2018-11-13 08:33:34 UTC |

~~Andrej Nemec~~ 2016-10-25 08:29:11 UTC Description

```
The `curl_getdate` converts a given date string into a
numerical timestamp and
it supports a range of different formats and possibilites to
express a date
and time. The underlying date parsing function is also used
internally when
parsing for example HTTP cookies (possibly received from
remote servers) and
it can be used when doing conditional HTTP requests.

The date parser function uses the libc sscanf() function at
two places, with
the parsing strings "%02d:%02d" and ""%02d:%02d:%02d". The
intent being that
it would parse either a string with HH:MM (two digits colon
two digits) or
HH:MM:SS (two digits colon two digits colon two digits). If
instead the piece
of time that was sent in had the final digit cut off, thus
ending with a
single-digit, the date parser code would advance its read
pointer one byte too
much and end up reading out of bounds.

External References:

https://curl.haxx.se/docs/adv_20161102G.html
```

~~Andrej Nemec~~ 2016-10-25 09:00:20 UTC Comment 1

```
Created attachment 1213777 [details]
Upstream patch
```

~~Adam Mariš~~ 2016-11-02 08:28:19 UTC Comment 2

```
Created curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1390894~~]
```

~~Adam Mariš~~ 2016-11-02 08:28:34 UTC Comment 3

```
Created mingw-curl tracking bugs for this issue:

Affects: fedora-all [~~bug 1390895~~]
Affects: epel-7 [~~bug 1390896~~]
```

errata-xmlrpc 2018-08-16 16:07:23 UTC Comment 6

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 08:33:18 UTC Comment 7

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.