



## Bug 1408385 (CVE-2016-9594) - CVE-2016-9594 curl: Unitialized random

**Keywords:** Security

**Status:** CLOSED NOTABUG

**Alias:** CVE-2016-9594

**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:**

**Blocks:**

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

**Reported:** 2016-12-23 08:33 UTC by Andrej Nemeec

**Modified:** 2021-02-17 02:50 UTC ([History](#))

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

**Fixed In Version:** curl 7.52.1

**Clone Of:**

**Environment:**

**Last Closed:** 2016-12-23 08:34:22 UTC

**Embargoed:**

**Attachments** ([Terms of Use](#))

Andrej Nemeec 2016-12-23 08:33:06 UTC

[Description](#)

libcurl's (new) internal function that returns a good 32bit random value was implemented poorly and overwrote the pointer instead of writing the value into the buffer the pointer pointed to.

This random value is used to generate nonces for Digest and NTLM authentication, for generating boundary strings in HTTP formposts and more. Having a weak or virtually non-existent random there makes these operations vulnerable.

This function is brand new in 7.52.0

## External References:

[https://curl.haxx.se/docs/adv\\_20161223.html](https://curl.haxx.se/docs/adv_20161223.html)

## Upstream patch:

<https://curl.haxx.se/CVE-2016-9594.patch>

Andrej Nemeec 2016-12-23 08:33:34 UTC

[Comment 1](#)

## Acknowledgments:

Name: Kamil Dudka (Red Hat)

Andrej Nemeec 2016-12-23 08:34:22 UTC

[Comment 2](#)

Vulnerable version is not shipped anywhere across our products.

## Note

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

