



☆ Starred by 1 user

Owner: jdeblasio@chromium.org

CC: mea...@chromium.org
 mgiuca@chromium.org
 creis@chromium.org

Status: Fixed (Closed)

Components: [UI>Security>UrlFormatting](#)

Modified: Sep 21, 2020

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: [Linux](#), [Android](#), [Windows](#), [Chrome](#), [Mac](#)

Pri: 2

Type: [Bug-Security](#)

[reward-0](#)
[Security_Severity-Low](#)
[Security_Impact-Stable](#)
[allpublic](#)
[CVE_description-submitted](#)
[Release-0-M85](#)
[CVE-2020-6571](#)
[Team-Security-UX](#)
[Team-TrustyTransport](#)

Issue 1085315: URL spoofing using 'GURMUKHI LETTER RRA' (U+0A5C)

Reported by rayya...@gmail.com on Thu, May 21, 2020, 12:32 AM EDT

🔗 Code

Steps to reproduce the problem:
Copy and Paste <http://163.com> (<http://www.xn--16-ogg.com/>)

163.com is in the list of top domains here, https://cs.chromium.org/chromium/src/components/url_formatter/spoof_checks/top_domains/domains.list

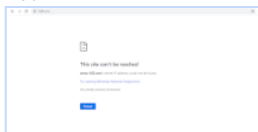
What is the expected behavior?
It should be converted into punycode

What went wrong?
Showed as it is.

Multiple examples from the top 10k domains:

103.by
13.cl
360.com

Spoofed.png
18.5 KB [View](#) [Download](#)



[Comment 1](#) by kenrb@chromium.org on Thu, May 21, 2020, 1:30 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: jdeblasio@chromium.org
Cc: mea...@chromium.org
Labels: [Security_Impact-Stable](#) [Security_Severity-Low](#) [OS-Android](#) [OS-Chrome](#) [OS-Linux](#) [OS-Mac](#) [OS-Windows](#)
Components: [UI>Security>UrlFormatting](#)

Thanks for the report.

[jdeblasio@](#): Can you take a look, since you had taken on [issue-906453](#) which is related?

[Comment 2](#) by [sheriffbot](#) on Thu, May 21, 2020, 2:50 PM EDT Project Member

Labels: [Pri-2](#)

Setting Pri-2 to match security severity Low. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

[Comment 3](#) by [bugdroid](#) on Thu, May 21, 2020, 6:19 PM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+c9733311e0cbb1687a3233c345640fe5fa9388f0>

commit [c9733311e0cbb1687a3233c345640fe5fa9388f0](#)

Author: Joe DeBlasio <jdeblasio@chromium.org>

Date: Thu May 21 22:16:25 2020

[IDN Spoof Checks] Add U+0A5C to digit lookalikes.

This CL adds U+0A5C as a lookalike character to the digit 3. This change appears to impact no domains seen in UKM.

~~Fixed-1086346~~

Change-Id: [lea9930363d853f154e2d781646a1b0b5da7fbbfd](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2212807>

Auto-Submit: Joe DeBlasio <jdeblasio@chromium.org>

Reviewed-by: Mustafa Emre Acer <meacer@chromium.org>

Commit-Queue: Joe DeBlasio <jdeblasio@chromium.org>

Cr-Commit-Position: refs/heads/master@{#771217}

[modify] https://crrev.com/c9733311e0cbb1687a3233c345640fe5fa9388f0/components/url_formatter/spoof_checks/idn_spoof_checker.cc

[Comment 4](#) by jdeblasio@chromium.org on Thu, May 21, 2020, 6:44 PM EDT Project Member

I added this character to the list since it had ~no impact on other sites and we've added worse, but I want to flag that I don't find this a particularly compelling spoof.

See attached. This is fairly close to how it's rendered across platforms.

Screen Shot 2020-05-21 at 3.42.38 PM.png

6.0 KB [View](#) [Download](#)



[Comment 5](#) by [sheriffbot](#) on Sun, May 24, 2020, 3:00 PM EDT Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

[Comment 6](#) by natashapabrai@google.com on Tue, May 26, 2020, 10:46 AM EDT Project Member

Labels: reward-topanel

[Comment 7](#) by natashapabrai@google.com on Fri, May 29, 2020, 1:10 PM EDT Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel declined to award this report.

[Comment 8](#) by adetaylor@google.com on Mon, Aug 24, 2020, 1:38 PM EDT Project Member

Labels: Release-0-M85

[Comment 9](#) by adetaylor@google.com on Mon, Aug 24, 2020, 3:29 PM EDT Project Member

Labels: CVE-2020-6571 CVE_description-missing

[Comment 10](#) by [sheriffbot](#) on Fri, Aug 28, 2020, 3:03 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit <https://www.chromium.org/issue-tracking/autotriage> - Your friendly Sheriffbot

[Comment 11](#) by adetaylor@google.com on Mon, Sep 21, 2020, 3:05 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted