





☆ Starred by 2 users

Owner:	 <a href="#">knollr@chromium.org</a> Not actively on Chrome anymore
CC:	 <a href="#">sangwoo108@chromium.org</a> <a href="#">adetaylor@chromium.org</a>  <a href="#">benmason@chromium.org</a> <a href="#">est...@chromium.org</a> <a href="#">pbomm...@chromium.org</a> <a href="#">ellyj...@chromium.org</a>  <a href="#">sarraf@chromium.org</a> <a href="#">achuith@chromium.org</a>
Status:	Fixed (Closed)
Components:	<a href="#">UI&gt;Browser&gt;Sharing</a>
Modified:	Mar 12, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	<a href="#">Linux, Windows, Chrome</a>
Pri:	1
Type:	<a href="#">Bug-Security</a>
<a href="#">Hotlist-Merge-Review</a> <a href="#">reward-2000</a> <a href="#">Security_Impact-Stable</a> <a href="#">Security_Severity-Medium</a> <a href="#">allpublic</a> <a href="#">reward-inprocess</a> <a href="#">CVE_description-submitted</a> <a href="#">Target-79</a> <a href="#">M-79</a> <a href="#">Merge-Rejected-79</a> <a href="#">Release-0-M80</a> <a href="#">CVE-2020-6397</a>	

Issue 1027408: Security: tel: URL scheme reference origin spoof on Windows and Linux  
Reported by [chrom...@gmail.com](#) on Thu, Nov 21, 2019, 11:51 PM EST

 Code

**VERSION**  
Chrome Version: 80.0.3973.4 canary  
Operating System: Windows and Linux

**REPRODUCTION CASE**

This is the same bug as [Issue 1095596](#) but I'm still able to repro it on Windows.

The sharing dialog will display on <https://www.apple.com/contact/> to call a number chosen by the attacker and in this case the victim would think that the '<https://www.apple.com/contact/>' is intended to make a call.

- On macOS, the sharing dialog disappears after the navigation.

**poc.html**  
147 bytes [View](#) [Download](#)

[Comment 1](#) Deleted

[Comment 2](#) Deleted

[Comment 3](#) Deleted

[Comment 4](#) by [chrom...@gmail.com](#) on Fri, Nov 22, 2019, 12:39 AM EST

**Recording #10.mp4**  
243 KB [View](#) [Download](#)



Comment 5 by [meacer@google.com](mailto:meacer@google.com) on Fri, Nov 22, 2019, 1:07 PM EST

**Status:** Assigned (was: Unconfirmed)

**Owner:** [knollr@chromium.org](mailto:knollr@chromium.org)

**Labels:** Security\_Severity-Medium Security\_Impact-Stable OS-Linux OS-Windows

**Components:** UI>Browser>Sharing

The previous fix ([crrev.com/c/1849382](https://crrev.com/c/1849382)) doesn't seem Mac specific so not sure why it doesn't help here. .

knollr: PTAL? Thanks!

Comment 6 by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Sat, Nov 23, 2019, 10:24 AM EST

**Labels:** Pri-1

Setting Pri-1 to match security severity Medium. 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 7 by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Sun, Nov 24, 2019, 9:46 AM EST

**Labels:** Target-79 M-79

Setting milestone and target because of Security\_Impact=Stable and medium severity.

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

Comment 8 by [knollr@chromium.org](mailto:knollr@chromium.org) on Mon, Nov 25, 2019, 10:12 AM EST

**Status:** Started (was: Assigned)

**Cc:** [est...@chromium.org](mailto:est...@chromium.org) [sarraf@chromium.org](mailto:sarraf@chromium.org)

Thanks! I'm taking a look why this is different from the original fix.

Comment 9 by [knollr@chromium.org](mailto:knollr@chromium.org) on Mon, Nov 25, 2019, 11:03 AM EST

**Labels:** OS-Chrome

The scenario here is slightly different from the one in <https://bug.com/1095506>. This opens the dialog on the same origin, so we don't display the source origin in the dialog, and then navigates to a different origin. The dialog keeps open on Linux, Windows and CrOS, but closes on Mac, probably because of different implementations of the `RenderWidgetHostView` [1] ?

The external protocol dialog for non-tel links on Linux and Windows closes automatically as it is a modal view and uses `WebContentsModalDialogManager` [2].

Other dialogs that inherit from `BubbleDialogDelegateView` would also have the same behavior (they close on navigation to different origin on Mac only), e.g. the bookmarks bubble is simple to test for this.

Emily, do you know what the expected behavior here is? Specifically for this dialog, I think we should just close it. Should this apply to all dialogs when navigating to a different origin or is this a special case for the Click to Call dialog?

[1]: [https://cs.chromium.org/chromium/src/content/browser/renderer\\_host/render\\_widget\\_host\\_view\\_mac.mm?l=444&rc1=0ff2da3a87117be8cee1c1432fb2a6cb8408f4f2](https://cs.chromium.org/chromium/src/content/browser/renderer_host/render_widget_host_view_mac.mm?l=444&rc1=0ff2da3a87117be8cee1c1432fb2a6cb8408f4f2)

[2]: [https://cs.chromium.org/chromium/src/components/web\\_modal/web\\_contents\\_modal\\_dialog\\_manager.cc?l=135&rc1=82ee2f16eefe2f9cf8faa85708115b660eb17019](https://cs.chromium.org/chromium/src/components/web_modal/web_contents_modal_dialog_manager.cc?l=135&rc1=82ee2f16eefe2f9cf8faa85708115b660eb17019)

Comment 10 by [knollr@chromium.org](mailto:knollr@chromium.org) on Tue, Dec 3, 2019, 12:51 PM EST

**Cc:** [ellyj...@chromium.org](mailto:ellyj...@chromium.org)

CL up for review to close the Click to Call dialogs when navigating cross origin: <https://crrev.com/c/1948839>

Comment 11 by [est...@chromium.org](mailto:est...@chromium.org) on Wed, Dec 4, 2019, 11:55 AM EST

**Cc:** [sangwoo108@chromium.org](mailto:sangwoo108@chromium.org)

Comment 12 by [bugdroid](mailto:bugdroid) on Wed, Dec 4, 2019, 1:45 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+888f8247e6478c7858828f0805b404c55eef19f>

commit [888f8247e6478c7858828f0805b404c55eef19f](https://chromium.googlesource.com/chromium/src.git/+888f8247e6478c7858828f0805b404c55eef19f)

Author: Richard Knoll <[knollr@chromium.org](mailto:knollr@chromium.org)>

Date: Wed Dec 04 18:42:11 2019

Close `SharingDialogs` on main frame cross origin navigation

This closes `SharingDialogViews` when the main frame navigates to a different origin. Right now this only affects the `SharingDialog` and (for CrOS) the `IntentPickerBubbleView` but will be enabled for all subclasses of `LocationBarBubbleDelegateView` in a subsequent change.

[Bug-1097408](#)

Change-Id: [I07ca9ce55042265d85e56a84c5e43efa3cb026d0](https://chromium-review.googlesource.com/c/chromium/src/+1948839)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1948839>

Commit-Queue: Richard Knoll <[knollr@chromium.org](mailto:knollr@chromium.org)>

Reviewed-by: Elly Fong-Jones <[ellyjones@chromium.org](mailto:ellyjones@chromium.org)>

Reviewed-by: Emily Stark <[estark@chromium.org](mailto:estark@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#721565}

[modify] [https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/intent\\_picker\\_bubble\\_view.cc](https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/intent_picker_bubble_view.cc)  
[modify] [https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/location\\_bar/location\\_bar\\_bubble\\_delegate\\_view.cc](https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/location_bar/location_bar_bubble_delegate_view.cc)  
[modify] [https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/location\\_bar/location\\_bar\\_bubble\\_delegate\\_view.h](https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/location_bar/location_bar_bubble_delegate_view.h)  
[modify] [https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/sharing/click\\_to\\_call\\_browser\\_test.cc](https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/sharing/click_to_call_browser_test.cc)  
[modify] [https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/sharing/sharing\\_dialog\\_view.cc](https://crrev.com/888f8247e6478c7858828f0805b404c55eff19f/chrome/browser/ui/views/sharing/sharing_dialog_view.cc)

**Comment 13** by [knollr@chromium.org](mailto:knollr@chromium.org) on Thu, Dec 5, 2019, 4:59 AM EST

**Status:** Fixed (was: Started)

Fixed in 80.0.3986.0, it now closes the dialog after navigation on non-macOS as well.

**Comment 14** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Thu, Dec 5, 2019, 10:45 AM EST

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

**Comment 15** by [awhalley@chromium.org](mailto:awhalley@chromium.org) on Wed, Dec 11, 2019, 5:53 PM EST

**Labels:** reward-topanel

**Comment 16** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Thu, Dec 12, 2019, 11:06 AM EST

**Labels:** Merge-Request-79

Requesting merge to beta M79 because latest trunk commit (721565) appears to be after beta branch point (706915).

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

**Comment 17** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Thu, Dec 12, 2019, 11:09 AM EST

**Labels:** -Merge-Request-79 Hotlist-Merge-Review Merge-Review-79

This bug requires manual review. Request affecting a post-stable build

Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?  
- Chrome: <https://goto.google.com/chrome-release-branch-merge-guidelines>  
- Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: [benmason@](mailto:benmason@)(Android), [kariahda@](mailto:kariahda@)(iOS), [cindyb@](mailto:cindyb@)(ChromeOS), [govind@](mailto:govind@)(Desktop)

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

**Comment 18** by [govind@chromium.org](mailto:govind@chromium.org) on Thu, Dec 12, 2019, 1:24 PM EST

**Cc:** [adetaylor@chromium.org](mailto:adetaylor@chromium.org) [benmason@chromium.org](mailto:benmason@chromium.org) [pbbomm@chromium.org](mailto:pbbomm@chromium.org)

+[adetaylor@](mailto:adetaylor@) (Security TPM) for M79 merge review

This is severity medium, no merge to M79 unless it is really needed. We would like to minimize the merges for next respin to reduce risk if possible at all.

**Comment 19** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Thu, Dec 12, 2019, 1:47 PM EST

**Labels:** -Merge-Review-79 Merge-Rejected-79

Yep let's reject this merge. Sheriffbot wants to merge to "beta", which is currently the same as stable, so let's not.

**Comment 20** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Mon, Dec 16, 2019, 3:10 PM EST

**Labels:** -reward-topanel reward-unpaid reward-2000

\*\*\* Boilerplate reminders! \*\*\*

Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact [security-vrp@chromium.org](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

**Comment 21** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Tue, Dec 17, 2019, 3:07 PM EST

Congrats! The Panel decided to reward \$2,000 for this report

**Comment 22** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Dec 19, 2019, 11:59 AM EST

**Labels:** -reward-unpaid reward-inprocess

**Comment 23** by [adetaylor@google.com](mailto:adetaylor@google.com) on Thu, Dec 26, 2019, 11:25 AM EST

See also [issue-1036833](https://crbug.com/1036833) for a related problem which still remains even after this fix.

**Comment 24** by [adetaylor@google.com](mailto:adetaylor@google.com) on Sat, Feb 1, 2020, 8:13 PM EST

**Labels:** Release-0-M80

**Comment 25** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 3, 2020, 6:47 PM EST

**Labels:** CVE-2020-6397 CVE\_description-missing

**Comment 26** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 10, 2020, 4:37 PM EST

**Labels:** -CVE\_description-missing CVE\_description-submitted

**Comment 27** by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Mar 4, 2020, 1:44 PM EST

**Cc:** [achuith@chromium.org](mailto:achuith@chromium.org)

**Comment 28** by [sheriffbot](mailto:sheriffbot) on Thu, Mar 12, 2020, 2:02 PM EDT

**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

