



☆ Starred by 2 users


Owner:


dpenning@chromium.org


CC:


 karandeepb@chromium.org


 solomonkinard@chromium.org

 tbergquist@chromium.org

 dpenning@chromium.org

 connily@chromium.org

 collinbaker@chromium.org

 top-chrome-bugs@google.com

Status:

Fixed (Closed)

Components:

UI>Browser>TopChrome>TabStrip

Modified:

Nov 15, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Windows, Chrome

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review

reward-5000

Security_Impact-Stable

Deadline-Exceeded

Security_Severity-High

allpublic

reward-inprocess

CVE_description-submitted

Target-90

M-92

Target-91

Target-92

external_security_report

merge-merged-4430

merge-merged-90

FoundIn-91

merge-merged-4472

merge-merged-91


LTS-Merged-90

LTS-Security-90

merge-merged-4515

merge-merged-92

Issue 1209616: Security: OOB read when window is closed while a link is being dragged over the tab strip
Reported by [derce...@gmail.com](#) on Sun, May 16, 2021, 9:45 AM EDT

 Code

VULNERABILITY DETAILS

When dragging a link over the tab strip, if the window is closed, an OOB read can occur in the browser process. This is due to the fact that when the window is closed, each of the tabs will be closed first and the window itself will be closed a short time later. If a drag message is processed in between the time when the tabs are removed and the window is closed, an OOB read will occur in the tab vector.

VERSION

Chrome Version: Tested on 92.0.4510.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE

1. Install the attached extension.
2. Once installed, the extension will create a window with a single tab. Drag a link (e.g. a bookmark, or the URL shown in the omnibox) over the tab strip in that window. Ensure the drop arrow shown in the tab strip appears in the middle of the tab or to the right (i.e. dragging the item anywhere within the tab strip will work, except towards the very left edge of the window).
3. Five seconds after opening the window, the extension will close it. Providing the item being dragged is still over the tab strip, this should result in an out-of-bounds read in the browser process. You can verify that by going through these steps in an asan build.

Note that the effect here is somewhat dependent on timing (see the explanation below), so you may have to try a few times for it to work.

CREDIT INFORMATION

Reporter credit: David Erceg

asan_output_883324.txt

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

background.js

321 bytes [View](#) [Download](#)

manifest.json

159 bytes [View](#) [Download](#)

page.html

98 bytes [View](#) [Download](#)

page.js

56 bytes [View](#) [Download](#)

[Comment 1](#) by [sheriffbot](#) on Sun, May 16, 2021, 9:49 AM EDT [Project Member](#)

Labels: external_security_report

[Comment 2](#) by [derce...@gmail.com](#) on Sun, May 16, 2021, 9:56 AM EDT

When a window is closed, all of the tabs in that window are removed:

<https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/browser.cc;l=934;drc=46bbb9795fcc1934c6cfbec096764f888c4d400a>

Then, the window itself will be closed, through an asynchronous task:

<https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/browser.cc;l=1267;drc=46bbb9795fcc1934c6cfbec096764f888c4d400a>

Additionally, as part of a drag operation involving a link, an arrow will be shown at the location in the tab strip where the drop will occur, if completed.

As can be seen in TabStrip::GetDropBounds, the tab at the drop index will be retrieved and the index will be clamped, so that it's not larger than GetTabCount() - 1:

https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/views/tabs/tab_strip.cc;l=3380;drc=46bbb9795fcc1934c6cfbec096764f888c4d400a

However, when a window is in the process of being closed, it's possible for a drag message to be processed after all of the tabs in the window have been removed, but before the window itself has been closed. In that case, GetTabCount will return 0. That then means that the index passed to tab_at will be -1 and an out-of-bounds read will occur.

Because this issue is triggered when a window is closed, it is possible to trigger it via a webpage, however I think there are two reasons why that would be somewhat more difficult than triggering the issue using an extension:

1. The entire window needs to be closed. That then means that the webpage would likely need to be opened in a window by itself (so that closing the tab results in the entire window being closed).
2. The webpage would either need to have been opened by a script, or have no back/forward history entries. This is due to the fact that there are restrictions on when a page can call window.close:

https://source.chromium.org/chromium/chromium/src/+main:third_party/blink/renderer/core/frame/dom_window.cc;l=344;drc=d2047b5fb1da5e49ea1b6009eed130b357ac3e1

Comment 3 by [xinghulu@chromium.org](#) on Mon, May 17, 2021, 2:15 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: solomonkinard@chromium.org
Cc: tbergquist@chromium.org collinbaker@chromium.org karandeepb@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>TabStrip

Thanks for the report! Hopefully <https://bug.com/1109717#e14> will fix all these security issues by preventing extensions from modifying tab strip while a tab drag was in progress.

Comment 4 by [sheriffbot](#) on Mon, May 17, 2021, 12:47 PM EDT Project Member

Labels: M-90 Target-90

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 5 by [sheriffbot](#) on Wed, May 26, 2021, 12:21 PM EDT Project Member

Labels: -M-90 M-91 Target-91

Comment 6 by [sheriffbot](#) on Sun, May 30, 2021, 12:21 PM EDT Project Member

solomonkinard: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 7 by [sheriffbot](#) on Sun, Jun 13, 2021, 12:21 PM EDT Project Member

solomonkinard: Uh oh! This issue still open and hasn't been updated in the last 28 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 8 by [solomonkinard@chromium.org](#) on Tue, Jun 29, 2021, 2:01 PM EDT Project Member

In me queue, but will ask for others to look.

Comment 9 by [solomonkinard@chromium.org](#) on Tue, Jun 29, 2021, 4:46 PM EDT Project Member

Owner: ----
Cc: solomonkinard@chromium.org connily@chromium.org dpenning@chromium.org

Comment 10 by [adetaylor@google.com](#) on Thu, Jul 8, 2021, 3:43 PM EDT Project Member

Owner: solomonkinard@chromium.org
Components: UI>Browser>TopChrome>TabStrip

solomonkinard@, I'm sorry, but security bugs need to be assigned and actively worked on. Please could you consult with one of your colleagues and work out who would be best to take care of this, then actively reassign?

Comment 11 by [adetaylor@google.com](#) on Thu, Jul 8, 2021, 4:21 PM EDT Project Member

Labels: FoundIn-91

Setting FoundIn-91 to match Security_Impact-Stable. I have no additional information that this can be reproduced in M91. But this label will become important to Sheriffbot in the near future.

Comment 12 by [tbergquist@chromium.org](#) on Thu, Jul 8, 2021, 4:47 PM EDT Project Member

Owner: dpenning@chromium.org

This is one of the ones that dpenning@ and I are reviewing.

Comment 13 by [tbergquist@chromium.org](#) on Fri, Jul 9, 2021, 1:57 PM EDT Project Member

Labels: -OS-Mac

I can't reproduce this on Mac. The window close is blocked until the link drag ends.

Comment 14 by [tbergquist@chromium.org](#) on Fri, Jul 9, 2021, 1:58 PM EDT Project Member

That said I do have a fix that I'm pretty confident in, I just can't test it myself since I only have access to a Mac. We'll go ahead and land it.

Comment 15 by [Git Watcher](#) on Mon, Jul 12, 2021, 8:21 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+8c956ce0d96372940ec1702bbacec4b37cfa5357>

commit [8c956ce0d96372940ec1702bbacec4b37cfa5357](#)

Author: Taylor Bergquist <tbergquist@chromium.org>

Date: Tue Jul 13 00:20:43 2021

Handle an empty tabstrip in TabStrip::GetDropBounds.

[Bug-1200646](#)

Change-Id: I7687d004bd970f94d5909e6c5349e0599022cf5d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3017667>

Reviewed-by: Peter Boström <pbos@chromium.org>

Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>

Cr-Commit-Position: refs/heads/master@{#900744}

[modify] https://crrev.com/8c956ce0d96372940ec1702bbacec4b37cfa5357/chrome/browser/ui/views/tabs/tab_strip.cc

Comment 16 by [adetaylor@google.com](#) on Tue, Jul 13, 2021, 9:59 PM EDT Project Member

derceg86@ do you think you'd be kind enough to test this fix once it appears in Canary?

tbergquist@ - please could you mark it as Fixed if you believe it's likely to be a complete fix, so that Sheriffbot can do all the merge requests - <https://chromium.googlesource.com/chromium/src/+refs/heads/main/docs/security/security-labels.md#TOC-Merge-labels>. Thanks!

Comment 17 by [tbergquist@chromium.org](#) on Wed, Jul 14, 2021, 2:59 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 18 by [sheriffbot](#) on Thu, Jul 15, 2021, 9:06 AM EDT Project Member

Labels: reward-topanel

Comment 19 by [sheriffbot](#) on Thu, Jul 15, 2021, 9:10 AM EDT Project Member

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

Comment 20 by [sheriffbot](#) on Thu, Jul 15, 2021, 9:11 AM EDT Project Member

Labels: Merge-Request-92 Merge-Request-91

Requesting merge to stable M91 because latest trunk commit (900744) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (900744) appears to be after beta branch point (885287).

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

Comment 21 by [sheriffbot](#) on Thu, Jul 15, 2021, 9:13 AM EDT Project Member

Labels: -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: We are only 4 days from stable.

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://chromium.googlesource.com/chromium/src.git/+main/docs/process/merge_request.md#when-to-request-a-merge
- 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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:

8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: <http://go/cros-engprodcomponents>

Please contact the milestone owner if you have questions.

Owners: govind@ (Android), benmason@ (iOS), dgagnon@ (ChromeOS), srinivassista@ (Desktop)

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

Comment 22 by [adetaylor@google.com](#) on Thu, Jul 15, 2021, 2:40 PM EDT Project Member

We should get more bake time before merging to M92 - we should consider merging to M92 in a while to pick it up in a security refresh.

Comment 23 by [derce...@gmail.com](#) on Thu, Jul 15, 2021, 9:29 PM EDT

Re #c16: I've tested a bit in Canary and the fix seems to work well.

Comment 24 by [amyressler@google.com](#) on Thu, Jul 22, 2021, 1:05 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 with any questions.

Comment 25 by [amyressler@google.com](#) on Thu, Jul 22, 2021, 1:12 PM EDT Project Member

Congrats, David! The VRP Panel has decided to award you \$5000 for this report. Another good one!

Comment 26 by [amyressler@google.com](#) on Fri, Jul 23, 2021, 1:25 PM EDT Project Member

Labels: -Merge-Request-91 -Merge-Review-92 Merge-Approved-92 Merge-Approved-91

Approved for merge to M92, please merge to branch 4515 at your earliest convenience.

Also approving merge to M91 as this has become the Extended Stable release branch; please merged to branch 4472 as well. Thank you!

Comment 27 by amyressler@google.com on Fri, Jul 23, 2021, 6:20 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 28 by srinivassista@google.com on Thu, Jul 29, 2021, 3:30 PM EDT Project Member

Status: Assigned (was: Fixed)

re-opening to get engineer attention for the merge

Please merge to M92 asap (before EOD thursday July 29)

Comment 29 by dpenning@chromium.org on Thu, Jul 29, 2021, 4:09 PM EDT Project Member

Cherry picked <https://chromium-review.googlesource.com/c/chromium/src/+3017667> to M92

Comment 30 by Git Watcher on Thu, Jul 29, 2021, 6:15 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+0bf00317ed3ada8009d62e0ce3c39eb144b8589>

commit 0bff00317ed3ada8009d62e0ce3c39eb144b8589

Author: Taylor Bergquist <tbergquist@chromium.org>

Date: Thu Jul 29 22:14:33 2021

Handle an empty tabstrip in TabStrip::GetDropBounds.

(cherry picked from commit 8c956ce0d96372940ec1702bbacec4b37cfa5357)

~~Bug-1200646~~

Change-Id: I7687d004bd970f94d5909e6c5349e0599022cf5d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3017667>

Reviewed-by: Peter Boström <pbos@chromium.org>

Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#900744}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3061458>

Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>

Commit-Queue: David Pennington <dpenning@chromium.org>

Cr-Commit-Position: refs/branch-heads/4515@{#1918}

Cr-Branched-From: 488fc70865ddaa05324ac0a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/0bff00317ed3ada8009d62e0ce3c39eb144b8589/chrome/browser/ui/views/tabs/tab_strip.cc

Comment 31 by amyressler@chromium.org on Fri, Jul 30, 2021, 9:57 AM EDT Project Member

Hello dpenning@, as this issue was discovered in M91, could you please merge to M91 branch 4472, asap for this issue to be a part of the extended stable release since we are moving toward a 4W stable release cycle. Thanks you!

Comment 32 by pbos@chromium.org on Fri, Jul 30, 2021, 12:28 PM EDT Project Member

I'll take care of the merge, David's out today.

Comment 33 by sheriffbot on Fri, Jul 30, 2021, 1:46 PM EDT Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 34 by Git Watcher on Fri, Jul 30, 2021, 2:02 PM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+f1e13ea0f18645899c534d15ed88c9ddf40b23d3>

commit f1e13ea0f18645899c534d15ed88c9ddf40b23d3

Author: Taylor Bergquist <tbergquist@chromium.org>

Date: Fri Jul 30 18:01:28 2021

Handle an empty tabstrip in TabStrip::GetDropBounds.

(cherry picked from commit 8c956ce0d96372940ec1702bbacec4b37cfa5357)

(cherry picked from commit 0bff00317ed3ada8009d62e0ce3c39eb144b8589)

~~Bug-1200646~~

Change-Id: I7687d004bd970f94d5909e6c5349e0599022cf5d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3017667>

Reviewed-by: Peter Boström <pbos@chromium.org>

Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>

Cr-Original-Original-Commit-Position: refs/heads/master@{#900744}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3061458>

Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>

Commit-Queue: David Pennington <dpenning@chromium.org>

Cr-Original-Commit-Position: refs/branch-heads/4515@{#1918}

Cr-Original-Branched-From: 488fc70865ddaa05324ac0a54a6eb783b4bc41c-refs/heads/master@{#885287}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3062679>

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Commit-Queue: Peter Boström <pbos@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#1586}

Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/f1e13ea0f18645899c534d15ed88c9ddf40b23d3/chrome/browser/ui/views/tabs/tab_strip.cc

Comment 35 by amyressler@chromium.org on Mon, Aug 2, 2021, 10:36 AM EDT Project Member

Labels: Release-1-M92

Comment 36 by amyressler@google.com on Mon, Aug 2, 2021, 10:57 AM EDT Project Member

Labels: CVE-2021-30593 CVE_description-missing

Comment 37 by sheriffbot on Thu, Aug 5, 2021, 1:42 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 38 by sheriffbot on Fri, Aug 6, 2021, 12:22 PM EDT Project Member

Labels: -release-1-m92 -Security_Impact-Extended

This bug is a regression and does not impact stable. Removing incorrectly added Release- labels.

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

Comment 39 by sheriffbot on Fri, Aug 6, 2021, 12:28 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 40 by amyressler@google.com on Fri, Aug 6, 2021, 1:07 PM EDT Project Member

Status: Fixed (was: Assigned)

Labels: Release-1-M92

Closing as fixed as this was bug was reopened (in comment # 28) by release team to gain attention for merge, which has been achieved. Need to get the bot to stop removing valid labels.

Comment 41 by sheriffbot on Sat, Aug 7, 2021, 12:21 PM EDT Project Member

Labels: -release-1-m92 -Security_Impact-Extended

This bug is a regression and does not impact stable. Removing incorrectly added Release- labels.

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

Comment 42 by sheriffbot on Sat, Aug 7, 2021, 12:25 PM EDT Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines:

<https://chromium.googlesource.com/chromium/src/+refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues> FoundIn guidelines:

https://chromium.googlesource.com/chromium/src/+main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 43 by sheriffbot on Sat, Aug 7, 2021, 12:25 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 44 by adetaylor@google.com on Sat, Aug 7, 2021, 4:51 PM EDT Project Member

Status: Fixed (was: Assigned)

Labels: Release-1-M92

Apologies for label change spam - this was a bug in our changes to make Sheriffbot work with the Extended Stable branch.

Comment 45 by rzanoni@google.com on Tue, Aug 10, 2021, 8:57 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 46 by sheriffbot on Tue, Aug 10, 2021, 12:21 PM EDT Project Member

Labels: -M-91 Target-92 M-92

Comment 47 by gianluca@google.com on Fri, Aug 20, 2021, 3:34 AM EDT Project Member

Labels: LTS-Merge-Approved-90

Comment 48 by gianluca@google.com on Fri, Aug 20, 2021, 3:36 AM EDT Project Member

Labels: -LTS-Merge-Request-90

Comment 49 by Git Watcher on Mon, Aug 23, 2021, 7:58 AM EDT Project Member

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+916bf13dd983af62491c68ea1b6a39f8de6f65a6>

commit 916bf13dd983af62491c68ea1b6a39f8de6f65a6

Author: Taylor Bergquist <tbergquist@chromium.org>

Date: Mon Aug 23 11:57:31 2021

[M90-LTS] Handle an empty tabstrip in TabStrip::GetDropBounds.

(cherry picked from commit [8c956ce0d96372940ec1702bbace04b37cfa5357](https://chromium.googlesource.com/chromium/src/+8c956ce0d96372940ec1702bbace04b37cfa5357))

~~bug-1200646~~

Change-Id: I7687d004bd970f94d5909e6c5349e0599022cfd5d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3017667>

Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#900744}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3085325>

Reviewed-by: Artem Sumaneev <asumaneev@google.com>

Owners-Override: Artem Sumaneev <asumaneev@google.com>

Commit-Queue: Roger Felipe Zanon da Silva <rzanoni@google.com>

Cr-Commit-Position: refs/branch-heads/4430@{#1573}

Cr-Branch-From: e5ce7dc4f7518237b3d9bb93ccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/916bf13dd983af62491c68ea1b6a39f8de6f65a6/chrome/browser/ui/views/tabs/tab_strip.cc

Comment 50 by rzanoni@google.com on Mon, Aug 23, 2021, 8:00 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 51 by amyressler@google.com on Thu, Aug 26, 2021, 1:09 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 52 by sheriffbot on Mon, Nov 15, 2021, 1:35 PM EST 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

