


☆ Starred by 3 users

Owner:

solomonkinard@chromium.org

CC:

rdevl...@chromium.org
tbergquist@chromium.org
connily@chromium.org
adetaylor@google.com
 collinbaker@chromium.org
dfried@chromium.org

Status:

Fixed (Closed)

Components:

Modified:

Aug 26, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

[Linux, Windows, Chrome, Mac](#)

Pri:

1

Type:

[Bug-Security](#)

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
M-90
Target-90
merge-merged-4240
LTS-Security-86
external_security_report
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
merge-merged-4430_101
Release-3-M90
CVE-2021-30509

Issue 1196309: Security: OOB vector insertion when extension highlights tab during drag

Reported by derce...@gmail.com on Tue, Apr 6, 2021, 12:15 PM EDT

 Code

VULNERABILITY DETAILS

When the user is dragging a tab, if an extension highlights another tab in the same tab strip, an out-of-bounds vector insertion will occur in the browser process when the user drags the tab past the last tab in the tab strip.

VERSION

Chrome Version: Tested on 89.0.4389.114 (stable) and 91.0.4469.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE

1. Install the attached extension.
2. Start dragging a tab in a window that has at least two tabs. When the extension detects that a tab has moved (using `chrome.tabs.onMoved`), it will mark one of the other tabs in the window as highlighted using the following call:

```
chrome.tabs.update(secondTab.id, {highlighted: true});
```

3. Drag the tab towards the right end of the tab strip (just past the halfway point of the last tab). This will result in an out-of-bounds vector insertion in the browser process.

Note that the demonstration is designed to make it easy to see when the issue is triggered, but an extension wouldn't necessarily have to rely on the user dragging a tab all the way to the right.

If you uncomment the last section in `background.js`, the extension will also move all the other tabs in the window to a new window (using `chrome.tabs.group`). That then means that dragging the active tab a little to the right will tend to trigger the issue, since there will only be two tabs left in the window (the tab being dragged and the tab the extension highlighted).

CREDIT INFORMATION

Reporter credit: David Erceg

asan_output_869515.txt
13.6 KB [View](#) [Download](#)

background.js
1.9 KB [View](#) [Download](#)

manifest.json
167 bytes [View](#) [Download](#)

[Comment 1](#) by [sheriffbot](#) on Tue, Apr 6, 2021, 12:20 PM EDT

Labels: external_security_report

[Comment 2](#) by derce...@gmail.com on Tue, Apr 6, 2021, 12:20 PM EDT

The direct cause of this issue is that the `to_position` value being passed to `TabStripModel::MoveWebContentsAtImpl` is one more than the size of the `contents_data_vector`. That method can be found at:

https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/ui/tabs/tab_strip_model.cc;_id=2011;drc=50802788094d7cf18b4682924e7249a6449b3238

The `to_position` value is then used to insert into the vector:

https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/ui/tabs/tab_strip_model.cc;_id=2022;drc=50802788094d7cf18b4682924e7249a6449b3238

The asan log attached in the initial message indicates an out-of-bounds read. This has to do with the fact that to insert an item in the middle of a vector (which this insertion is treated as, due to the invalid iterator), `libc++` first moves item forwards while traversing backwards through them.

However, because the insertion point here is past the end of the vector, the code ends up traversing back past the start of the vector (which is why the asan log indicates the read is to the left of the vector). This can then cause heap corruption, from having adjacent portions of memory overwritten.

Comment 3 by cthomp@chromium.org on Tue, Apr 6, 2021, 5:48 PM EDT

Status: Assigned (was: Unconfirmed)

Owner: dfried@chromium.org

Labels: Security_Severity-High Security_Impact-Stable M-89 OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1

Components: UI>Browser>TabStrip

Thanks for the report and the additional investigation! This is a clever attack vector -- I've previously considered other cases where an extension might be able to interact with TabStrip lifetimes/etc. but not with the highlighting API. This does trigger an OOB write in the browser process, but it requires a malicious extension and user interaction to trigger, so I'm marking this Severity-High.

[dfried@](mailto:dfried@chromium.org) could you take a look or help assign this to someone on the desktop UI team or `chrome/browser/ui/tabs/OWNERS`?

Comment 4 by cthomp@chromium.org on Thu, Apr 8, 2021, 2:21 PM EDT

[Issue-1197146](#) is a similar (but different root cause) bug exploiting the interaction between the `chrome.tabs` API and TabStrip features, from the same reporter. As mentioned there, I think we should look into doing some variant analysis here as well. Happy to coordinate Security assisting with that effort.

Comment 5 by cthomp@chromium.org on Thu, Apr 8, 2021, 5:06 PM EDT

Owner: tbergquist@chromium.org

Cc: dfried@chromium.org connilly@chromium.org

Per <https://bugs.chromium.org/p/chromium/issues/detail?id=1197146#c3> re-assigning this to [tbergquist@](mailto:tbergquist@chromium.org). Thanks!

Comment 6 by connilly@chromium.org on Tue, Apr 13, 2021, 2:01 PM EDT

Owner: collinbaker@chromium.org

Cc: tbergquist@chromium.org

Comment 7 by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT

Labels: -M-89 M-90 Target-90

Comment 8 by sheriffbot on Tue, Apr 20, 2021, 12:21 PM EDT

collinbaker: 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 9 by collinbaker@chromium.org on Tue, Apr 20, 2021, 3:22 PM EDT

Owner: rdevl...@chromium.org

Cc: collinbaker@chromium.org

I can repro this with a browser test (i.e. without using an extension): <https://chromium-review.googlesource.com/c/chromium/src/+2841209>

I think this is a design bug rather than an implementation bug. `TabDragController` assumes the tab selection does not change while dragging. Ignoring extensions, this holds true: the selection only changes (AFAIK) when the user CTRL+ or SHIFT+ clicks tabs. But this cannot happen while dragging.

I see two options here:

1. Redesign `TabDragController` to support tab selection changes while dragging.
2. Block tab selection changes from `chrome.tabs` during dragging.

(1) seems like an enormous task, with limited benefit. (2) seems much more reasonable to me.

Also, do we know how many extensions rely on modifying tab selection?

Devlin: can you give input on whether (2) is reasonable, or tag someone who'd know? I'm not sure who, if anyone, owns the `chrome.tabs` API.

Comment 10 by rdevl...@chromium.org on Tue, Apr 20, 2021, 3:42 PM EDT

Owner: solomonkinard@chromium.org

Cc: rdevl...@chromium.org

> Also, do we know how many extensions rely on modifying tab selection?

Nope, and unfortunately, this isn't something we could easily determine.

> Devlin: can you give input on whether (2) is reasonable

(2) sounds very reasonable to me. Even more than just while dragging, I almost think disallowing updates to selection while any tabs are selected seems reasonable - having an extension override your selection sounds kind of undesirable.

[solomonkinard@](mailto:solomonkinard@chromium.org), is this something you have the bandwidth to tackle?

Additional questions: Do we know if there's similar issues with moving tabs while dragging? What about if the extension either a) moves one of the selected tabs to a non-contiguous location or b) inserts a non-selected tab into a selected group? I wouldn't be surprised if we had similar badness (even if not a security bug, perhaps a functional bug or safe crash).

Comment 11 by collinbaker@chromium.org on Tue, Apr 20, 2021, 3:53 PM EDT

> Additional questions: Do we know if there's similar issues with moving tabs while dragging? What about if the extension either a) moves one of the selected tabs to a non-contiguous location or b) inserts a non-selected tab into a selected group? I wouldn't be surprised if we had similar badness (even if not a security bug, perhaps a functional bug or safe crash).

Not aware of bugs filed for these specifically, but here are similar bugs related to `chrome.tabs` updates while dragging:

[Issue-1198747](#) (pin tag while dragging)

Issue 1197888 (duplicating a group tab while dragging)

[Issue-1197146](#) (moving tabs between groups while dragging)

Comment 12 by solomonkinard@chromium.org on Tue, Apr 20, 2021, 3:53 PM EDT

Status: Started (was: Assigned)

Sure, I can take a look.

Comment 13 by rdevlin@chromium.org on Tue, Apr 20, 2021, 5:31 PM EDT

ooh, fun! Thanks for highlighting those, collinbaker@. And thank you for all the great finds, derceg86@ :)

collinbaker@ + solomonkinard@, please coordinate here to make sure we don't duplicate any effort, since it seems like there are a few of these touching the same bits of code.

Comment 14 Deleted

Comment 15 by solomonkinard@chromium.org on Wed, Apr 28, 2021, 2:08 AM EDT

crrev.com/c/2849068

Comment 16 by [Git Watcher](#) on Thu, Apr 29, 2021, 3:28 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+4220923a7a20b136b61d10098975046e0f6bda9>

commit 4220923a7a20b136b61d10098975046e0f6bda9

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Thu Apr 29 19:27:01 2021

[Extensions][Tabs] OOB when extension highlights tab during drag

The bug includes an existing test that was incorporated into this CL.

This was tested via the included test and manually with two extensions.

One extension uses tabs.update(highlighted) and the other uses

tab.highlight(). Those tests haven't been included in this CL for

faster turnaround.

[Bug-1106300](#)

Change-Id: I591e411f82abb6e70567882d4eaf6c99d08ab51

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2849068>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Reviewed-by: Collin Baker <collinbaker@chromium.org>

Reviewed-by: Collin Baker <collinbaker@google.com>

Cr-Commit-Position: refs/heads/master@{#877593}

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/extensions/api/tabs/tabs_api.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/extensions/api/tabs/tabs_constants.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/extensions/api/tabs/tabs_constants.h

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/browser_tab_strip_model_delegate.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/browser_tab_strip_model_delegate.h

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/tabs/tab_strip_model.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/tabs/tab_strip_model.h

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/tabs/tab_strip_model_delegate.h

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_ui_test.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/views/tabs/tab_strip.cc

[modify] https://crrev.com/4220923a7a20b136b61d10098975046e0f6bda9/chrome/browser/ui/views/tabs/tab_strip.h

Comment 17 by solomonkinard@chromium.org on Thu, Apr 29, 2021, 4:01 PM EDT

Status: Fixed (was: Started)

Comment 18 by solomonkinard@chromium.org on Thu, Apr 29, 2021, 4:14 PM EDT

M90 crrev.com/c/2859232

M91: crrev.com/c/2860567

Comment 19 by solomonkinard@chromium.org on Thu, Apr 29, 2021, 9:39 PM EDT

Labels: Merge-Request-91 Merge-Request-90

Comment 20 by solomonkinard@chromium.org on Thu, Apr 29, 2021, 9:40 PM EDT

Added due to preexisting labels: M-90, Target-90

Comment 21 by [sheriffbot](#) on Fri, Apr 30, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 22 by [sheriffbot](#) on Fri, Apr 30, 2021, 2:02 PM EDT

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

Comment 23 by [sheriffbot](#) on Fri, Apr 30, 2021, 3:30 PM EDT

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review

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/+master/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: benmason@(Android), bindusuvama@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

[Comment 24](#) by [Git Watcher](#) on Fri, Apr 30, 2021, 11:09 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+112a415ce3ee8252c7bc62fe68883aee101c7cc1>

commit [112a415ce3ee8252c7bc62fe68883aee101c7cc1](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Sat May 01 03:08:50 2021

[Extensions][Tabs] Use IsTabStripEditable() as CanHighlight abstraction

This addresses comments on crrev.com/c/2849068. Another benefit is it starts to address one of the TODOs that pbs@ wants to look into later regarding terms like highlight and selected.

[Bug-1106300](#)

Change-Id: Icb45ab7c696056e4f4560cd424ae928a22f28482

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2860874>

Reviewed-by: Karan Bhatia <karandeepb@chromium.org>

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

Reviewed-by: Connie Wan <connily@chromium.org>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

Cr-Commit-Position: refs/heads/master@{#878203}

[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/browser_tab_strip_model_delegate.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/browser_tab_strip_model_delegate.h
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/tabs/tab_strip_model_delegate.h
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/views/tabs/tab_strip.cc
[modify] https://crrev.com/112a415ce3ee8252c7bc62fe68883aee101c7cc1/chrome/browser/ui/views/tabs/tab_strip.h

[Comment 25](#) by adetaylor@google.com on Mon, May 3, 2021, 11:22 AM EDT

Labels: -Merge-Request-90 -Merge-Review-91 Merge-Approved-90 Merge-Approved-91

Approving merge to M90, branch 4430, and M91 branch 4472. (My read of the comments that resulted in [#c24](#) are that they are purely about naming, etc. and don't functionally affect the patch, so there's no need to merge the patch in [#c24](#). Let me know if I'm reading that wrong).

[Comment 26](#) by pbommana@google.com on Tue, May 4, 2021, 7:08 AM EDT

[Bulk Edit] Your change has been approved for M91. Please go ahead and merge the CL to branch 4472 (refs/branch-heads/4472) manually asap so that it would be part of tomorrow's Beta release.

[Comment 27](#) by solomonkinard@chromium.org on Tue, May 4, 2021, 1:18 PM EDT

We might want to consider merging in that patch and others later, but you're right that it doesn't change the behavior with or without it.

[Comment 28](#) by [sheriffbot](#) on Thu, May 6, 2021, 12:13 PM EDT

Cc: adetaylor@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 29](#) by [Git Watcher](#) on Thu, May 6, 2021, 3:57 PM EDT

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+9a9dd29ee89ab56ce133080abb057971822858f4>

commit [9a9dd29ee89ab56ce133080abb057971822858f4](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Thu May 06 19:55:58 2021

[M90][Extensions][Tabs] OOB when extension highlights tab during drag

The bug includes an existing test that was incorporated into this CL.

This was tested via the included test and manually with two extensions.

One extension uses tabs.update(highlighted) and the other uses tab.highlight(). Those tests haven't been included in this CL for faster turnaround.

[Bug-1106300](#)

(cherry picked from commit [4220923a7a20b136b61d10098975046e0f6bdaf9](#))

Change-Id: I591e411f82abb6e70567882d4eaf6c99d08ab51

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2849068>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Devlin <devlin.cronin@chromium.org>

Reviewed-by: Collin Baker <collinbaker@chromium.org>

Reviewed-by: Collin Baker <collinbaker@google.com>

Cr-Original-Commit-Position: refs/heads/master@{#877593}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2859232>

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

Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>

Cr-Commit-Position: refs/branch-heads/4430@{#1414}

Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#875950}

[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/browser_tab_strip_model_delegate.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/browser_tab_strip_model_delegate.h

[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/tabs/tab_strip_model.h
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/tabs/tab_strip_model_delegate.h
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_uiitest.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/views/tabs/tab_strip.cc
[modify] https://crrev.com/9a9dd29ee89ab56ce133080abb057971822858f4/chrome/browser/ui/views/tabs/tab_strip.h

Comment 30 by [Git Watcher](#) on Thu, May 6, 2021, 4:48 PM EDT

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+2a7d8380b75558f036ed58f13b4bd282cdfa2ab0>

commit [2a7d8380b75558f036ed58f13b4bd282cdfa2ab0](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Thu May 06 20:47:56 2021

[M91][Extensions][Tabs] OOB when extension highlights tab during drag

The bug includes an existing test that was incorporated into this CL.

This was tested via the included test and manually with two extensions.

One extension uses tabs.update(highlighted) and the other uses tab.highlight(). Those tests haven't been included in this CL for faster turnaround.

[Bug-1106300](#)

(cherry picked from commit [4220923a7a20b136b61d10098975046e0f6bda9](#))

Change-Id: I591e411f82abb6e70567882d4eaf6c99d08ab51

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2849068>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Reviewed-by: Collin Baker <collinbaker@chromium.org>

Reviewed-by: Collin Baker <collinbaker@google.com>

Cr-Original-Commit-Position: refs/heads/master@{#877593}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2860567>

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

Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#802}

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

[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/browser_tab_strip_model_delegate.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/browser_tab_strip_model_delegate.h
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/tabs/tab_strip_model.h
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/tabs/tab_strip_model_delegate.h
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_uiitest.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/views/tabs/tab_strip.cc
[modify] https://crrev.com/2a7d8380b75558f036ed58f13b4bd282cdfa2ab0/chrome/browser/ui/views/tabs/tab_strip.h

Comment 31 by amyressler@chromium.org on Fri, May 7, 2021, 5:25 PM EDT

Labels: Release-3-M90

Comment 32 by vsavu@google.com on Mon, May 10, 2021, 9:20 AM EDT

Labels: LTS-Merge-Request-86 LTS-Security-86

Comment 33 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT

Labels: CVE-2021-30509 CVE_description-missing

Comment 34 by gianluca@google.com on Wed, May 12, 2021, 12:33 PM EDT

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 35 by [Git Watcher](#) on Wed, May 12, 2021, 12:50 PM EDT

Labels: merge-merged-4240

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+23ce88849f979b1f0b56b29dab500e599a9eb2d2>

commit [23ce88849f979b1f0b56b29dab500e599a9eb2d2](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Wed May 12 16:49:34 2021

[M86-LTS][Extensions][Tabs] OOB when extension highlights tab during drag

The bug includes an existing test that was incorporated into this CL.

This was tested via the included test and manually with two extensions.

One extension uses tabs.update(highlighted) and the other uses tab.highlight(). Those tests haven't been included in this CL for faster turnaround.

[M86]: Resolved conflicts due to missing code.

[Bug-1106300](#)

(cherry picked from commit [4220923a7a20b136b61d10098975046e0f6bda9](#))

Change-Id: I591e411f82abb6e70567882d4eaf6c99d08ab51

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2849068>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Devlin <devlin.cronin@chromium.org>
Reviewed-by: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Collin Baker <collinbaker@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#877593}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2883624>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuth@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1632}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/browser_tab_strip_model_delegate.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/browser_tab_strip_model_delegate.h
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/tabs/tab_strip_model_delegate.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/tabs/tab_strip_model_delegate.h
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_ui_test.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/views/tabs/tab_strip.cc
[modify] https://crrev.com/23ce88849f979b1f0b56b29dab500e599a9eb2d2/chrome/browser/ui/views/tabs/tab_strip.h

Comment 36 by amyressler@google.com on Wed, May 12, 2021, 7:11 PM EDT

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 37 by amyressler@chromium.org on Wed, May 12, 2021, 7:22 PM EDT

Congratulations, David! The VRP Panel has decided to award you \$10,000 for this report. Excellent work!

Comment 38 by amyressler@google.com on Mon, May 17, 2021, 2:21 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 39 by Git Watcher on Mon, May 17, 2021, 3:29 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+33109f1824b9ae3d488b7372f9aca68f611be606>

commit 33109f1824b9ae3d488b7372f9aca68f611be606

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Mon May 17 19:28:43 2021

[Extensions][Tabs] Ensure tab strip is editable before editing

Bug: [1109747, 1107146](#), 1197888, [1106300, 1202508](#)

Change-Id: Icf51669a7f7b17a35cd2c0ed018abcfedf068a26

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2891080>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Karan Bhatia <karandeepb@chromium.org>

Cr-Commit-Position: refs/heads/master@{#883567}

[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/test/base/test_browser_window.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/test/base/test_browser_window.h

Comment 40 by solomonkinard@chromium.org on Mon, May 17, 2021, 3:54 PM EDT

crrev.com/c/2891080 merged.

Comment 41 by Git Watcher on Tue, May 18, 2021, 8:10 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+f5ae8693fcb042797de12b6b9cc055da0090a80a>

commit f5ae8693fcb042797de12b6b9cc055da0090a80a

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Wed May 19 00:09:39 2021

[M91][Extensions][Tabs] Ensure tab strip is editable before editing

(cherry picked from commit 33109f1824b9ae3d488b7372f9aca68f611be606)

Bug: [1109747, 1107146](#), 1197888, [1106300, 1202508](#)

Change-Id: Icf51669a7f7b17a35cd2c0ed018abcfedf068a26

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2891080>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Karan Bhatia <karandeepb@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#883567}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2904568>

Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#11619}

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

[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc

[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/test/base/test_browser_window.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/test/base/test_browser_window.h

Comment 42 by [Git Watcher](#) on Wed, May 19, 2021, 3:42 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+/?260804a2f0823fdec95e69de0e449bb9fed1f35>

commit [7260804a2f0823fdec95e69de0e449bb9fed1f35](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Wed May 19 19:41:28 2021

[Extensions][Tabs] Include error message if not model isn't editable

See crrev.com/c/2904568.

~~Bug-1108717, 1107146, 1197888, 1106300, 1202508~~

Change-Id: [Idc6f1a1e336e08926de75226debcff799d703d00](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+?2903572>

Reviewed-by: Karan Bhatia <karandeepb@chromium.org>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

Cr-Commit-Position: refs/heads/master@{#884626}

[modify] https://crrev.com/7260804a2f0823fdec95e69de0e449bb9fed1f35/chrome/browser/extensions/api/tabs/tabs_api.cc

Comment 43 by [Git Watcher](#) on Thu, May 20, 2021, 7:02 AM EDT

Labels: merge-merged-4430_101

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+?ce3c9a1aa475591cf3a0664498e9ebd89f38b84e>

commit [ce3c9a1aa475591cf3a0664498e9ebd89f38b84e](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Thu May 20 10:59:16 2021

[M90][Extensions][Tabs] OOB when extension highlights tab during drag

The bug includes an existing test that was incorporated into this CL.

This was tested via the included test and manually with two extensions.

One extension uses `tabs.update(highlighted)` and the other uses

`tab.highlight()`. Those tests haven't been included in this CL for

faster turnaround.

~~Bug-1106300~~

(cherry picked from commit [4220923a7a20b136b61d10098975046e0f6bdaf9](#))

(cherry picked from commit [9a9dd29ee89ab56ce13308abb057971822858f4](#))

Change-Id: [I591e411f82abb6e70567882d4eaf6c9d08ab51](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+?2849068>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Reviewed-by: Collin Baker <collinbaker@chromium.org>

Reviewed-by: Collin Baker <collinbaker@google.com>

Cr-Original-Commit-Position: refs/heads/master@{#877593}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+?2859232>

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

Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>

Cr-Original-Commit-Position: refs/branch-heads/4430@{#1414}

Cr-Original-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@{#857950}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+?2884094>

Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>

Owners-Override: Victor-Gabriel Savu <vsavu@google.com>

Cr-Commit-Position: refs/branch-heads/4430_101@{#46}

Cr-Branched-From: [3e9034a21f4b1f6707146b1309e001c3321ab48a](#)-refs/branch-heads/4430@{#1364}

Cr-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@{#857950}

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/extensions/api/tabs/tabs_api.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/extensions/api/tabs/tabs_constants.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/extensions/api/tabs/tabs_constants.h

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/browser_tab_strip_model_delegate.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/browser_tab_strip_model_delegate.h

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/tabs/tab_strip_model.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/tabs/tab_strip_model.h

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/tabs/tab_strip_model_delegate.h

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/tabs/test_tab_strip_model_delegate.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/tabs/test_tab_strip_model_delegate.h

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_uiitest.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/views/tabs/tab_strip.cc

[modify] https://crrev.com/ce3c9a1aa475591cf3a0664498e9ebd89f38b84e/chrome/browser/ui/views/tabs/tab_strip.h

Comment 44 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT

Labels: -CVE, -description-missing CVE, -description-submitted

Comment 45 by [Git Watcher](#) on Wed, Jun 9, 2021, 11:56 AM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+?7aeb825dc9b93ba302d1c124c572213c4967b53>

commit [7aeb825dc9b93ba302d1c124c572213c4967b53](#)

Author: Solomon Kinard <solomonkinard@chromium.org>

Date: Wed Jun 9 15:54:57 2021

[M90-LTS][Extensions][Tabs] Ensure tab strip is editable before editing

(cherry picked from commit 33109f1824b9ae3d488b7372f9aca68f611be606)

(cherry picked from commit f5ae8693fcb042797de12b6b9cc055da0090a80a)

~~bug-1408717,1407146,1197888,1406306,1202668~~

Change-Id: Ic51669a7f7b17a35cd2c0ed018abcfeddf068a26

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2891080>

Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>

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

Reviewed-by: Karan Bhatia <karandeepb@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#883567}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2904568>

Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>

Cr-Original-Commit-Position: refs/branch-heads/4472@{#1169}

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

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2944872>

Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>

Commit-Queue: Artem Sumaneev <asumaneev@google.com>

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

Cr-Commit-Position: refs/branch-heads/4430@{#1503}

Cr-Branched-From: e5ce7dc47f518237b3d9bb93ccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_api.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_constants.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_constants.h

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/extension_tab_util.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/extension_tab_util.h

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/test/base/test_browser_window.cc

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/test/base/test_browser_window.h

Comment 46 by sheriffbot on Thu, Aug 26, 2021, 1:30 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