☆ Starred by 2 users

Owner:	solomonkinard@chromium.org
CC:	karandeepb@chromium.org solomonkinard@chromium.org tbergquist@chromium.org cthomp@chromium.org
Status:	Fixed *(Closed)*
Components:	----
Modified:	Sep 15, 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
Target-90
M-91
LTS-Security-86
LTS-Security-NotApplicable-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
Release-0-M91
CVE-2021-30526

Issue 1198717: Security: OOB write after extension pins tab during drag

Reported by derce...@gmail.com on Tue, Apr 13, 2021, 6:55 PM EDT

Code

VULNERABILITY DETAILS
When the user is dragging a tab that was initially in a group, an extension can mark the tab as pinned. If the drag is then cancelled, the tab will be moved back into its original group, resulting in a tab that's both pinned and in a group. Moving the group to a different index will then also move the pinned tab. This then breaks the constraint that pinned tabs are always at the start of the tab strip. Finally, attempting to move the pinned tab to a different index will result in an out-of-bounds write in the browser process.

VERSION
Chrome Version: Tested on 92.0.4477.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE
1. Install the attached extension.
2. Move a tab into a new group, then start dragging the tab within its tab strip.
3. Once the extension detects that a tab has been moved (using chrome.tabs.onMoved), the extension will mark the tab as pinned and navigate it.
On Windows, the tab will be navigated to "mailto:". This will cause the drag to be cancelled, at least on Windows 10, when the application chooser dialog is shown.
On other platforms, the tab will be navigated to about:blank (simply to make it easy to tell when the drag should be cancelled) and you'll need to manually cancel the drag by pressing ESC.
The updated tab will now be both pinned and in a group.
4. Five seconds later, the extension will call chrome.tabGroups.move to move the group to index 1. This will move the pinned tab, meaning that there's now a pinned tab that's not at the start of the tab strip.
5. Finally, the extension will use chrome.tabs.move to move the pinned tab to index 0. This will result in an OOB write in the browser process.

CREDIT INFORMATION
Reporter credit: David Erceg

asan_output_872117.txt
11.3 KB View Download

manifest.json
196 bytes View Download

service_worker.js
1.1 KB View Download

Comment 1 by sheriffbot on Tue, Apr 13, 2021, 6:57 PM EDT Project Member

Labels: external_security_report

Comment 2 by derce...@gmail.com on Tue, Apr 13, 2021, 7:05 PM EDT

Ultimately, the end result of this issue is similar to the result described in ~~issue 1196309~~. However. the core problem here is that when a drag is cancelled, the group of each dragged tab is restored, regardless of whether or not any of the tabs have been pinned. That's something that's done at the end of TabDragController::RevertDragAt:

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/views/tabs/tab_drag_controller.cc;l=1742;drc=a9cc926063ef9fad68351d9c24d7e26b00c634c7

In this case, the to_position value passed to TabStripModel::MoveWebContentsAtImpl is -1 and the element is written just before the start of the contents_data_ vector.

Comment 3 by est...@chromium.org on Wed, Apr 14, 2021, 10:38 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: collinbaker@chromium.org
Cc: cthomp@chromium.org
Labels: Security_Impact-Stable Security_Severity-High M-89 OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>TabStrip

Triaging to match ~~issue 1196309~~ and friends

Comment 4 by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT Project Member

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

Comment 5 by collinbaker@chromium.org on Wed, Apr 21, 2021, 5:01 PM EDT Project Member

Cc: solomonkinard@chromium.org

Comment 6 by adetaylor@google.com on Thu, Apr 29, 2021, 12:58 PM EDT Project Member

collinbaker@ could we have an update here? This is getting fairly old for a High severity security bug.

Comment 7 by collinbaker@chromium.org on Thu, Apr 29, 2021, 2:23 PM EDT Project Member

solomonkinard@ is working on ~~issue 1196309~~ which is similar. We are waiting on that fix before proceeding with this.

Comment 8 by solomonkinard@chromium.org on Fri, Apr 30, 2021, 1:43 PM EDT Project Member

Owner: solomonkinard@chromium.org

Comment 9 by solomonkinard@chromium.org on Tue, May 4, 2021, 10:52 PM EDT Project Member

crrev.com/c/2873364

Comment 10 by solomonkinard@chromium.org on Wed, May 12, 2021, 1:47 PM EDT Project Member

Cc: karandeepb@chromium.org

cc cl reviewer

Comment 11 by karandeepb@chromium.org on Wed, May 12, 2021, 2:21 PM EDT Project Member

We decided to prevent the extensions code from modifying the tab strip while a tab drag was in progress to prevent these security issues. (Another CL: https://chromium-review.googlesource.com/c/chromium/src/+/2891080)

Can we add (or have we already added) some validation to the tab strip code as well to ensure clients don't modify the tab strip while a tab drag is in progress? Said differently, even if the extensions code tries to modify the tab strip during a tab drag, it shouldn't result in an out-of-bounds and the tab strip code should handle it gracefully (either the operation should be a no-op or result in a DCHECK failure I think, with the former preferred IMO).

Comment 12 by solomonkinard@chromium.org on Thu, May 13, 2021, 2:11 PM EDT Project Member

Cc: tbergquist@chromium.org

Comment 13 by Git Watcher on Mon, May 17, 2021, 3:29 PM EDT Project Member

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: 1198717~~,~~1197146~~,1197888,~~1196309~~,~~1202598~~
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-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 14 by solomonkinard@chromium.org on Mon, May 17, 2021, 3:50 PM EDT Project Member

Status: Fixed (was: Assigned)

crrev.com/c/2891080 merged.

Comment 15 by sheriffbot on Tue, May 18, 2021, 12:43 PM EDT Project Member

Labels: reward-topanel

Comment 16 by sheriffbot on Tue, May 18, 2021, 2:02 PM EDT Project Member

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

Comment 17 by sheriffbot on Tue, May 18, 2021, 2:23 PM EDT Project Member

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

Requesting merge to stable M90 because latest trunk commit (883567) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (883567) appears to be after beta branch point (965).

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

Comment 18 by sheriffbot on Tue, May 18, 2021, 2:26 PM EDT Project Member

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

This bug requires manual review: We are only 6 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/+/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), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 19 by adetaylor@google.com on Tue, May 18, 2021, 4:22 PM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91. Please merge to branch 4472. M91 stable cut is today, so this will almost certainly miss the initial release of M91, but we'll pick it up in the first stable refresh.

Comment 20 by solomonkinard@chromium.org on Tue, May 18, 2021, 4:32 PM EDT Project Member

Thanks.

Comment 21 by Git Watcher on Tue, May 18, 2021, 8:10 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/+/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: 1198717~~,~~1197146~~,1197888,~~1196309~~,~~1202508~~
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-Commit-Position: refs/branch-heads/4472@{#1169}
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 22 by Git Watcher on Wed, May 19, 2021, 3:42 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7260804a2f0823fdec95e69de0e449bb9fed1f35

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: 1198717~~,~~1197146~~,1197888,~~1196309~~,~~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 23 by adetaylor@google.com on Fri, May 21, 2021, 3:43 PM EDT Project Member

Labels: -Merge-Request-90

Comment 24 by amyressler@chromium.org on Mon, May 24, 2021, 11:07 AM EDT Project Member

Labels: Release-0-M91

Comment 25 by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT Project Member

Labels: CVE-2021-30526 CVE_description-missing

Comment 26 by janag...@google.com on Wed, May 26, 2021, 10:57 AM EDT Project Member

Cc: janag...@google.com
Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 27 by janag...@google.com on Wed, May 26, 2021, 11:17 AM EDT Project Member
Labels: -LTS-Merge-Request-86 LTS-Security-NotApplicable-86

Not applicable to LTS since tab groups API was added after LTS branch.

Comment 28 by janag...@google.com on Wed, May 26, 2021, 11:38 AM EDT Project Member
Cc: -janag...@google.com

Comment 29 by amyressler@google.com on Wed, Jun 2, 2021, 3:51 PM EDT Project Member
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 30 by amyressler@chromium.org on Thu, Jun 3, 2021, 5:50 PM EDT Project Member

Congrats, David on another one! The VRP panel has decided to award you $10,000 for this report.

Comment 31 by amyressler@google.com on Fri, Jun 4, 2021, 10:50 AM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 32 by asumaneev@google.com on Mon, Jun 7, 2021, 3:11 PM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 33 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 34 by sheriffbot on Tue, Jun 8, 2021, 12:21 PM EDT Project Member
Labels: -M-90 M-91 Target-91

Comment 35 by gianluca@google.com on Wed, Jun 9, 2021, 10:43 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 36 by Git Watcher on Wed, Jun 9, 2021, 11:56 AM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7aeab825dc9b93ba302d1c124c572213c4967b53

```
commit 7aeab825dc9b93ba302d1c124c572213c4967b53
Author: Solomon Kinard <solomonkinard@chromium.org>
Date: Wed Jun 09 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: 1198717~~,~~1197146~~,1197888,~~1196309~~,~~1202598~~

```
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-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: Achuith 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: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-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 37 by asumaneev@google.com on Wed, Jun 9, 2021, 11:57 AM EDT Project Member
Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 38 by sheriffbot on Wed, Sep 15, 2021, 1:31 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