☆ Starred by 5 users

Owner:	cyan@chromium.org OOO
CC:	solomonkinard@chromium.org pbos@chromium.org tbergquist@chromium.org collinbaker@chromium.org amyressler@chromium.org top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>TabStrip>TabGroups
Modified:	Sep 30, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
Target-90
M-91
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
Release-0-M92
CVE-2021-30565
LTS-Size-Small

Issue 1210985: Security: OOB write after moving pinned tab into a group

Reported by derce...@gmail.com on Wed, May 19, 2021, 2:02 PM EDT

Code

VULNERABILITY DETAILS
A pinned tab typically can't be placed in a group. However, when using the Ctrl+Shift+PgUp/Ctrl+Shift+PgDn shortcuts (to move a tab to the previous/next position; only supported on Linux and Chrome OS Lacros), the selected tab will be added to an adjacent group, if there is one. That's true even if the selected tab is pinned.

An extension with the debugger permission can then use this behavior to produce the same effect as described in ~~issue 1108717~~ and ~~issue 1200460~~. Specifically, moving the group will also move the pinned tab, breaking the constraint that pinned tabs are always at the start of the tab strip. Then, 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 92.0.4513.0 (latest asan build)
Operating System: Ubuntu 20.04.2

REPRODUCTION CASE
1. Install the attached extension.
2. Once installed, the extension will create a window with two tabs and add one of those tabs to a group.
3. It will then create a pinned tab, attach the debugger to it and use Input.dispatchKeyEvent to dispatch the Ctrl+Shift+PgDn shortcut to it. As the pinned tab is located directly before the tab that was grouped, the pinned tab will be added to that group.
4. The extension will then call chrome.tabGroups.move to move the group to the end of the tab strip. This will also 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_884517.txt
12.7 KB View Download

manifest.json
213 bytes View Download

service_worker.js
1.7 KB View Download

Comment 1 by sheriffbot on Wed, May 19, 2021, 2:06 PM EDT Project Member

Labels: external_security_report

Comment 2 by derce...@gmail.com on Wed, May 19, 2021, 2:07 PM EDT

The core issue here is that TabStripModel::MoveTabRelative doesn't check whether a tab is pinned when determining whether it should be added to an adjacent group:

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/tabs/tab_strip_model.cc;l=2011;drc=46bbb9795fcc1934c6cfbec096764f888c4d400a

Also, as stated in the summary, the Ctrl+Shift+PgUp/Ctrl+Shift+PgDn shortcuts are only supported on Linux and Chrome OS Lacros:

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/views/accelerator_table.cc;l=68-70;drc=8e734c8346bd17a5752fbd4f82f3156d67635edf

So this issue is only relevant on those platforms.

Comment 3 by vakh@chromium.org on Sat, May 22, 2021, 2:46 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: solomonkinard@chromium.org
Cc: collinbaker@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Linux OS-Lacros
Components: UI>Browser>TabStrip

Thanks for the bug report.
Triaging to match ~~issue 1209469~~.

M90: crash/9d3c8c73ccbc233e
M91: crash/5ed9ce4c865dd486

Comment 4 by sheriffbot on Sat, May 22, 2021, 12:46 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 Sat, May 22, 2021, 1:27 PM EDT Project Member

Labels: -Pri-3 Pri-1

Setting Pri-1 to match security severity High. 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 6 by sheriffbot on Wed, May 26, 2021, 12:21 PM EDT Project Member

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

Comment 7 by sheriffbot on Thu, Jun 3, 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 8 by collinbaker@chromium.org on Thu, Jun 3, 2021, 4:42 PM EDT Project Member

Owner: cyan@chromium.org
Cc: solomonkinard@chromium.org tbergquist@chromium.org

As described in #c2 the core issue is that TabStripModel allows pinned tabs to be moved into a group without being unpinned.

Routing to Charlene who worked on dragging into groups and dragging to pin/unpin, since this seems related. Also tagging Taylor who has related tab strip knowledge.

Comment 9 by Git Watcher on Thu, Jun 10, 2021, 6:16 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/05198700faf344500e765218ca96b161b010fc45

commit 05198700faf344500e765218ca96b161b010fc45
Author: Charlene Yan <cyan@chromium.org>
Date: Thu Jun 10 22:15:34 2021

[Tab Groups] Cap boundaries so tabs can't be moved across {un}/pinned.

~~Bug: 1210985~~
Change-Id: I211c42703ebb384d019e1c8cda3d055d034e8492
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2945337
Commit-Queue: Charlene Yan <cyan@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Commit-Position: refs/heads/master@{#891409}

[modify] https://crrev.com/05198700faf344500e765218ca96b161b010fc45/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/05198700faf344500e765218ca96b161b010fc45/chrome/browser/ui/tabs/tab_strip_model_unittest.cc

Comment 10 by cyan@chromium.org on Wed, Jun 16, 2021, 8:14 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 11 by sheriffbot on Thu, Jun 17, 2021, 12:43 PM EDT Project Member

Labels: reward-topanel

Comment 12 by sheriffbot on Thu, Jun 17, 2021, 2:03 PM EDT Project Member

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

Comment 13 by sheriffbot on Thu, Jun 17, 2021, 2:23 PM EDT Project Member

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

Requesting merge to stable M91 because latest trunk commit (891409) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (891409) appears to be after beta branch point (885287).

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

Comment 14 by sheriffbot on Thu, Jun 17, 2021, 2:27 PM EDT Project Member

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

This bug requires manual review: M92'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: govind@(Android), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 15 by srinivassista@google.com on Thu, Jun 17, 2021, 3:05 PM EDT Project Member

pls answer comment #14 for merge-review.

Comment 16 by srinivassista@google.com on Mon, Jun 21, 2021, 1:32 PM EDT Project Member

Friendly ping ^

Comment 17 by srinivassista@google.com on Tue, Jun 22, 2021, 12:59 PM EDT Project Member

Status: Assigned (was: Fixed)

re-opening to get engineer attention for merge to M92

Comment 18 by cyan@chromium.org on Wed, Jun 23, 2021, 1:26 PM EDT Project Member

Cc: pbos@chromium.org

Comment 19 by cyan@chromium.org on Wed, Jun 23, 2021, 3:47 PM EDT Project Member

Just tested this on ToT and it did not crash.

1. This is a high severity OOB write bug.
2. https://chromium-review.googlesource.com/c/chromium/src/+/2945337
3. Yes
4. This was introduced in M85.
5. Found security bug.
6. No.

Comment 20 by amyressler@chromium.org on Wed, Jun 23, 2021, 4:13 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 21 by amyressler@chromium.org on Wed, Jun 23, 2021, 4:15 PM EDT Project Member

Labels: -Merge-Review-92 Merge-Approved-92

merge approved for M92, please merge to branch 4515 asap. Thanks!!

Comment 22 by Git Watcher on Wed, Jun 23, 2021, 5:19 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/+/4e8d756caa45baf0465a69cbd4f49ceaf6628e45

commit 4e8d756caa45baf0465a69cbd4f49ceaf6628e45
Author: Charlene Yan <cyan@chromium.org>
Date: Wed Jun 23 21:18:19 2021

[Tab Groups] Cap boundaries so tabs can't be moved across {un}/pinned.

(cherry picked from commit 05198700faf344500e765218ca96b161b010fc45)

~~Bug: 1210985~~
Change-Id: I211c42703ebb384d019e1c8cda3d055d034e8492
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2945337
Commit-Queue: Charlene Yan <cyan@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#891409}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2983652
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#962}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/4e8d756caa45baf0465a69cbd4f49ceaf6628e45/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/4e8d756caa45baf0465a69cbd4f49ceaf6628e45/chrome/browser/ui/tabs/tab_strip_model_unittest.cc

Comment 23 by amyressler@chromium.org on Wed, Jun 23, 2021, 6:17 PM EDT Project Member

Components: UI>Browser>TopChrome>TabStrip>TabGroups

Comment 24 by amyressler@google.com on Wed, Jun 23, 2021, 7:24 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-15000

*** 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@chromium.org on Wed, Jun 23, 2021, 7:26 PM EDT Project Member

Congratulations, David. The VRP Panel has decided to reward you $15000 for this report. Nice work as per usual!

Comment 26 by amyressler@chromium.org on Mon, Jun 28, 2021, 12:59 PM EDT Project Member

Labels: -Merge-Request-91 Merge-Approved-91

At this time there isn't another security refreshed planned for M91. Merge approved to M91 to prepare for any potential unplanned security refresh scenarios before M92.
Please merge to branch 4472 at your convenience. Thanks!

Comment 27 by amyressler@google.com on Wed, Jun 30, 2021, 5:38 PM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 28 by sheriffbot on Fri, Jul 2, 2021, 12:15 PM EDT Project Member
Cc: amyressler@chromium.org

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 amyressler@chromium.org on Mon, Jul 19, 2021, 3:12 PM EDT Project Member
Labels: Release-0-M92

Comment 30 by amyressler@google.com on Mon, Jul 19, 2021, 7:14 PM EDT Project Member
Labels: CVE-2021-30565 CVE_description-missing

Comment 31 by Git Watcher on Tue, Jul 27, 2021, 3:51 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/+/eac37c18783def1328257489f633e3f562e30cc0

commit eac37c18783def1328257489f633e3f562e30cc0
Author: Charlene Yan <cyan@chromium.org>
Date: Tue Jul 27 19:50:03 2021

[Tab Groups] Cap boundaries so tabs can't be moved across {un}/pinned.

(cherry picked from commit 05198700faf344500e765218ca96b161b010fc45)

(cherry picked from commit 4e8d756caa45baf0465a69cbd4f49ceaf6628e45)

~~Bug: 1210985~~
Change-Id: I211c42703ebb384d019e1c8cda3d055d034e8492
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2945337
Commit-Queue: Charlene Yan <cyan@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#891409}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2983652
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4515@{#962}
Cr-Original-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3003458
Cr-Commit-Position: refs/branch-heads/4472@{#1579}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/eac37c18783def1328257489f633e3f562e30cc0/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/eac37c18783def1328257489f633e3f562e30cc0/chrome/browser/ui/tabs/tab_strip_model_unittest.cc

Comment 32 by rzanoni@google.com on Thu, Jul 29, 2021, 6:07 AM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 33 by amyressler@google.com on Tue, Aug 3, 2021, 3:41 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 34 by gianluca@google.com on Thu, Aug 5, 2021, 6:23 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 35 by Git Watcher on Tue, Aug 17, 2021, 11:54 AM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3b96593da9517623119e4c5d501f4abd2d12acb6

commit 3b96593da9517623119e4c5d501f4abd2d12acb6
Author: Charlene Yan <cyan@chromium.org>
Date: Tue Aug 17 15:53:41 2021

[M90-LTS][Tab Groups] Cap boundaries so tabs can't be moved across {un}/pinned.

(cherry picked from commit 05198700faf344500e765218ca96b161b010fc45)

~~Bug: 1210985~~
Change-Id: I211c42703ebb384d019e1c8cda3d055d034e8492
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2945337
Commit-Queue: Charlene Yan <cyan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#891409}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3059451
Commit-Queue: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Jana Grill <janagrill@google.com>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Jana Grill <janagrill@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1566}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/3b96593da9517623119e4c5d501f4abd2d12acb6/chrome/browser/ui/tabs/tab_strip_model.cc
[modify] https://crrev.com/3b96593da9517623119e4c5d501f4abd2d12acb6/chrome/browser/ui/tabs/tab_strip_model_unittest.cc

Comment 36 by rzanoni@google.com on Wed, Aug 18, 2021, 3:43 AM EDT Project Member
Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 37 by sheriffbot on Thu, Sep 30, 2021, 1:29 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