☆ Starred by 3 users

Owner:	⏱ collinbaker@chromium.org **Last visit 17 days ago**
CC:	tbergquist@chromium.org connily@chromium.org adetaylor@google.com ⏱ top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>TabStrip>TabGroups
Modified:	Aug 26, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
M-90
Target-89
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-2021-30511
reward-11000
TopChrome

Issue 1197875: Security: OOB read when attempting to add tab to group after groups have changed
Reported by derce...@gmail.com on Sat, Apr 10, 2021, 4:23 PM EDT

🔗 | Code

VULNERABILITY DETAILS
The context menu shown for a tab allows that tab to be added to an existing group. However, if one or more groups were removed in the time since the menu was shown, an out-of-bounds read can occur in the browser process.

VERSION
Chrome Version: Tested on 92.0.4474.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE
1. Install the attached extension.
2. Once installed, the extension will create a new window with three tabs: two that are in a group and one that's not.
3. Right-click the tab that's not in a group.
4. Five seconds after opening the window, the extension will ungroup the second tab. Once this has happened, select the final entry from the "Add tab to group" submenu.
This will cause an out-of-bounds read in the browser process.

CREDIT INFORMATION
Reporter credit: David Erceg

    asan_output_871272.txt
    12.7 KB View Download

    background.js
    577 bytes View Download

    manifest.json
    163 bytes View Download

Comment 1 by derce...@gmail.com on Sat, Apr 10, 2021, 4:26 PM EDT
The issue here is that when a group is selected from the "Add tab to group" submenu, the ExistingTabGroupSubMenuModel::ExecuteExistingCommand method retrieves a list of current groups and attempts to retrieve the selection from that:

https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc;l=96;drc=3f97e29466e8450418d0897f2170 6ffc0d1aef20

However, the tab groups may have changed since the menu was first shown. This then means that the command_index value can be out-of-bounds.

A suggested patch is attached, which simply changes the DCHECK in that method to an early return (since it doesn't make sense to continue the method if command_index is out-of-bounds).

    suggested_patch.patch
    865 bytes View Download

Comment 2 by sheriffbot on Sat, Apr 10, 2021, 4:27 PM EDT   Project Member

Labels: external_security_report

[Comment 3](#) by cthomp@chromium.org on Mon, Apr 12, 2021, 6:31 PM EDT

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

Thanks as always for the clear report (and extra for the suggested patch!).

Confirmed repro on [r871272](#) ASAN. I can also repro on [r843829](#) ASAN.

Passing this one to tbergquist@ as well.

[Comment 4](#) by sheriffbot on Tue, Apr 13, 2021, 12:47 PM EDT
Labels: Target-89 M-89

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 connily@chromium.org on Tue, Apr 13, 2021, 2:01 PM EDT

Owner: collinbaker@chromium.org
Cc: tbergquist@chromium.org

[Comment 6](#) by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT
Labels: -M-89 M-90 Target-90

[Comment 7](#) by collinbaker@chromium.org on Tue, Apr 20, 2021, 4:56 PM EDT

Thank you for the detailed report and suggested patch. A fix is in progress at https://chromium-review.googlesource.com/c/chromium/src/+/2841823

[Comment 8](#) by Git Watcher on Tue, Apr 27, 2021, 6:14 PM EDT

Status: Fixed (was: Assigned)
The following revision refers to this bug:

  https://chromium.googlesource.com/chromium/src/+/65b5b467c8a57ece2ec782adda098ae07d48f205

commit [65b5b467c8a57ece2ec782adda098ae07d48f205](#)
Author: Collin Baker <[collinbaker@chromium.org](#)>
Date: Tue Apr 27 22:12:56 2021

Handle out-of-bounds group index when adding tab to existing group

~~Fixed: 1197875~~
Change-Id: I5b4749e8cec0ec1b00388f81504723acc01e4389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2841823
Auto-Submit: Collin Baker <[collinbaker@chromium.org](#)>
Reviewed-by: Taylor Bergquist <[tbergquist@chromium.org](#)>
Commit-Queue: Collin Baker <[collinbaker@chromium.org](#)>
Cr-Commit-Position: refs/heads/master@{#876785}

[modify] https://crrev.com/65b5b467c8a57ece2ec782adda098ae07d48f205/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/65b5b467c8a57ece2ec782adda098ae07d48f205/chrome/browser/ui/tabs/tab_menu_model_unittest.cc

[Comment 9](#) by sheriffbot on Wed, Apr 28, 2021, 12:42 PM EDT
Labels: reward-topanel

[Comment 10](#) by sheriffbot on Thu, Apr 29, 2021, 2:02 PM EDT
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

[Comment 11](#) by sheriffbot on Thu, Apr 29, 2021, 2:22 PM EDT
Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (876785) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (876785) appears to be after beta branch point (870763).

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

[Comment 12](#) by sheriffbot on Thu, Apr 29, 2021, 2:23 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), bindusuvarna@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

[Comment 13](#) by adetaylor@google.com on Mon, May 3, 2021, 11:11 AM EDT
Labels: -Merge-Request-90 -Merge-Review-91 Merge-Approved-90 Merge-Approved-91

Approving merge to M91, branch 4472, and M90, branch 4430.

[Comment 14](#) 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 15 by sheriffbot on Thu, May 6, 2021, 12:13 PM EDT   Project Member
  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 16 by pbommana@google.com on Thu, May 6, 2021, 11:00 PM EDT   Project Member

Please merge your change to M90 branch 4430 ASAP so we can pick it up for next M90 respin. Thank you.

Comment 17 by srinivassista@google.com on Fri, May 7, 2021, 2:19 PM EDT   Project Member
 Status: Assigned (was: Fixed)

Marking as assigned to get attention for the pending merge

Comment 18 by Git Watcher on Fri, May 7, 2021, 4:26 PM EDT   Project Member
 Status: Fixed (was: Assigned)
 Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/e8412ccab087da5ccc5ebb8de19071cd810e8460

commit e8412ccab087da5ccc5ebb8de19071cd810e8460
Author: Collin Baker <collinbaker@chromium.org>
Date: Fri May 07 20:25:16 2021

Handle out-of-bounds group index when adding tab to existing group

(cherry picked from commit 65b5b467c8a57ece2ec782adda098ae07d48f205)

Fixed: 1197875
Change-Id: I5b4749e8cec0ec1b00388f81504723acc01e4389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2841823
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#876785}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2880712
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1426}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/e8412ccab087da5ccc5ebb8de19071cd810e8460/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/e8412ccab087da5ccc5ebb8de19071cd810e8460/chrome/browser/ui/tabs/tab_menu_model_unittest.cc

Comment 19 by amyressler@chromium.org on Mon, May 10, 2021, 9:26 AM EDT   Project Member
 Labels: Release-3-M90

Comment 20 by vsavu@google.com on Mon, May 10, 2021, 9:29 AM EDT   Project Member
 Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 21 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT   Project Member
 Labels: CVE-2021-30511 CVE_description-missing

Comment 22 by pbommana@google.com on Mon, May 10, 2021, 11:18 AM EDT   Project Member

[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 this weeks Beta release.

Comment 23 by sheriffbot on Mon, May 10, 2021, 12:15 PM EDT   Project Member

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 24 by pbommana@google.com on Tue, May 11, 2021, 1:43 AM EDT   Project Member

collinbaker@ please get the change merged to M91 Branch asap.

Comment 25 by Git Watcher on Tue, May 11, 2021, 2:10 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/+/06bd45efd298107d2f53796287b18ae497e31646

commit 06bd45efd298107d2f53796287b18ae497e31646
Author: Collin Baker <collinbaker@chromium.org>
Date: Tue May 11 18:08:59 2021

Handle out-of-bounds group index when adding tab to existing group

(cherry picked from commit 65b5b467c8a57ece2ec782adda098ae07d48f205)

Fixed: 1197875
Change-Id: I5b4749e8cec0ec1b00388f81504723acc01e4389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2841823
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#876785}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2888185

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Peter Boström <pbos@chromium.org>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#943}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/06bd45efd298107d2f53796287b18ae497e31646/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/06bd45efd298107d2f53796287b18ae497e31646/chrome/browser/ui/tabs/tab_menu_model_unittest.cc

Comment 26 by gianluca@google.com on Wed, May 12, 2021, 12:32 PM EDT   Project Member
 Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 27 by Git Watcher on Wed, May 12, 2021, 12:48 PM EDT   Project Member
 Labels: merge-merged-4240

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/6d04816608feca6e7fabea7a469b5f4b480cb354

commit 6d04816608feca6e7fabea7a469b5f4b480cb354
Author: Collin Baker <collinbaker@chromium.org>
Date: Wed May 12 16:47:24 2021

[M86-LTS]: Handle out-of-bounds group index when adding tab to existing group

[M86]: Enabled feature in test.

(cherry picked from commit 65b5b467c8a57ece2ec782adda098ae07d48f205)

(cherry picked from commit e8412ccab087da5ccc5ebb8de19071cd810e8460)

Fixed: 1197875
Change-Id: I5b4749e8cec0ec1b00388f81504723acc01e4389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2841823
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#876785}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2880712
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1426}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883763
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1631}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/6d04816608feca6e7fabea7a469b5f4b480cb354/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/6d04816608feca6e7fabea7a469b5f4b480cb354/chrome/browser/ui/tabs/tab_menu_model_unittest.cc

Comment 28 by amyressler@google.com on Wed, May 12, 2021, 7:11 PM EDT   Project Member
 Labels: -reward-topanel reward-unpaid reward-11000

*** 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 29 by amyressler@chromium.org on Wed, May 12, 2021, 7:25 PM EDT   Project Member
Congratulations, David on another one! The VRP Panel has decided to award you $11,000 for this report + a patch bonus. Awesome stuff!

Comment 30 by amyressler@google.com on Mon, May 17, 2021, 2:21 PM EDT   Project Member
 Labels: -reward-unpaid reward-inprocess

Comment 31 by Git Watcher on Thu, May 20, 2021, 7:02 AM EDT   Project Member
 Labels: merge-merged-4430_101

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/1410f2e6927072f41424a85e64d36755b19d3d39

commit 1410f2e6927072f41424a85e64d36755b19d3d39
Author: Collin Baker <collinbaker@chromium.org>
Date: Thu May 20 10:59:16 2021

Handle out-of-bounds group index when adding tab to existing group

(cherry picked from commit 65b5b467c8a57ece2ec782adda098ae07d48f205)

(cherry picked from commit e8412ccab087da5ccc5ebb8de19071cd810e8460)

Fixed: 1197875
Change-Id: I5b4749e8cec0ec1b00388f81504723acc01e4389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2841823
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#876785}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2880712
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1426}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884106
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>

Cr-Commit-Position: refs/branch-heads/4430_101@{#53}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/1410f2e6927072f41424a85e64d36755b19d3d39/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/1410f2e6927072f41424a85e64d36755b19d3d39/chrome/browser/ui/tabs/tab_menu_model_unittest.cc

Comment 32 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT   Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 33 by sheriffbot on Thu, Aug 26, 2021, 1:30 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

About Monorail   User Guide   Release Notes   Feedback on Monorail   Terms   Privacy