bugs chromium New issue Open issues Search chromium issue Sign in

☆ Starred by 3 users

Owner:	dlja...@chromium.org
CC:	dpenning@chromium.org sky@chromium.org top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>TabStrip>TabGroups
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-2000
M-100
Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
Hotlist-Merge-Approved
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
Target-100
FoundIn-99
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1491
TopChrome

Issue 1305706: uaf in BookmarkBarView::OnTabGroupButtonPressed

Reported by wxhu...@gmail.com on Sat, Mar 12, 2022, 7:58 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.51 Safari/537.36

Steps to reproduce the problem:
1.a
2.
3.

What is the expected behavior?

What went wrong?
a

Did this work before? N/A

Chrome version: 99.0.4844.51 Channel: stable
OS Version: 10.0

uaf.txt
21.8 KB View Download

Comment 1 by sheriffbot on Sat, Mar 12, 2022, 8:03 AM EST

Labels: external_security_report

Comment 2 by wxhu...@gmail.com on Sat, Mar 12, 2022, 8:19 AM EST

1. open one tab and save as a tab group
2. open anathor tab and save as anathor tab group
3. you can see two tab group button in your bookmark view bar
4.move one of group to anathor tab group, (just let your chrome has one tab group)
5.click the old one tab group button of bookview bar.
6. uaf occur.

Comment 3 Deleted

Comment 4 by wxhu...@gmail.com on Sat, Mar 12, 2022, 9:13 AM EST

my chromium commit is a20ff7247d590579a7c93cdbb2c577db30b92226

Comment 5 Deleted

Comment 6 by wxhu...@gmail.com on Sun, Mar 13, 2022, 3:06 AM EDT

forget to say that you shoule enable "#tab-groups-save"

Comment 7 by bookholt@chromium.org on Mon, Mar 14, 2022, 5:18 PM EDT

Owner: sky@chromium.org
Labels: Security_Severity-Medium FoundIn-99
Components: UI>Browser>TopChrome>TabStrip>TabGroups

I'm not able to reproduce this bug, although I may not be interpreting comment #2 correctly, so I'll pass along to the subsystem owner for a second opinion.

If this is reachable, it would appear to require the user to perform a precise sequence of UI actions to trigger. Therefore, assigning Medium Severity as the highest possible applicable security severity level.

Comment 8 by sheriffbot on Mon, Mar 14, 2022, 5:19 PM EDT

Labels: Security_Impact-Stable

Comment 9 by sky@chromium.org on Mon, Mar 14, 2022, 11:26 PM EDT

Owner: dlja...@chromium.org
Cc: sky@chromium.org

Comment 10 by dljames@google.com on Tue, Mar 15, 2022, 12:08 AM EDT

Thank you for the bug! This issue is currently being worked on. Will add updates here as soon I get them 👍

Comment 11 by dlja...@chromium.org on Tue, Mar 15, 2022, 1:04 PM EDT

Cc: dpenning@chromium.org

Comment 12 by dpenning@chromium.org on Tue, Mar 15, 2022, 1:15 PM EDT

wxhusst@gmail.com can you please provide more specific repro for the step
"4.move one of group to anathor tab group, (just let your chrome has one tab group)"

Comment 13 by dlja...@chromium.org on Tue, Mar 15, 2022, 2:31 PM EDT

These are the steps I did to reproduce this bug:

1. Enable the #tab-groups-save feature
2. Create 2 tab groups (Does not matter how many tabs are in them)
3. Save both tab groups
   > You should see 2 new buttons appear in the bookmarks bar with the names of the saved tab groups.
4. Click on the first tab group that was saved
   > Will be the leftmost tab group button if the default Left to right mode is enabled.
   > Will be the right most tab group button if Right to left mode enabled.

Please let me know if there are any differences between these steps and the ones described above!

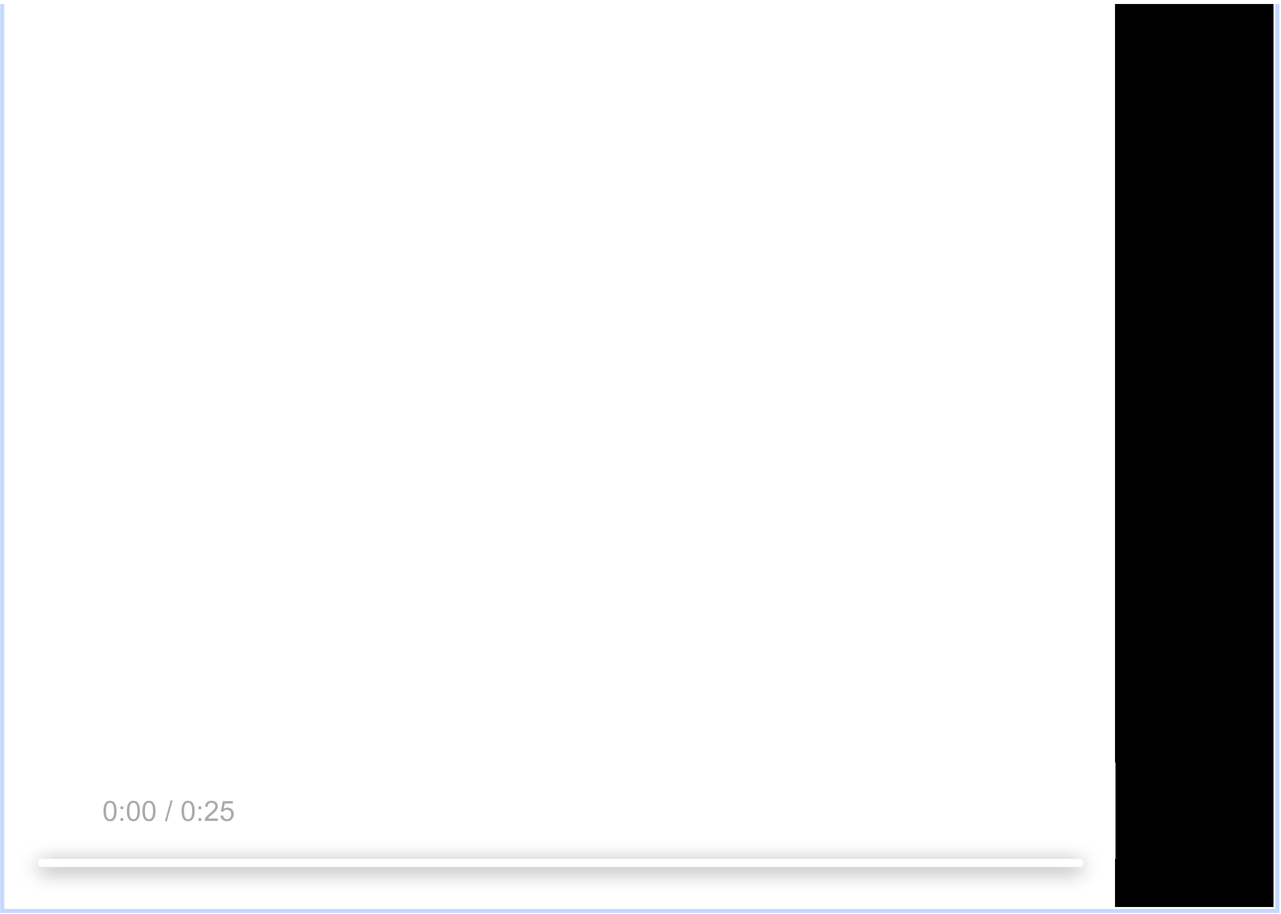
Comment 14 by wxhu...@gmail.com on Wed, Mar 16, 2022, 3:32 AM EDT

I will upload a video. Sorry for my bad English

Comment 15 by wxhu...@gmail.com on Wed, Mar 16, 2022, 8:01 AM EDT

poc1.mp4

11.4 MB View Download



uaf.txt
23.4 KB View Download

Comment 16 by dljames@google.com on Wed, Mar 16, 2022, 12:03 PM EDT

No worries! Thank you for the video, this is perfect!

Comment 17 by dpenning@chromium.org on Wed, Mar 16, 2022, 12:22 PM EDT

we should probably go back to design and ask what we should do when there isnt any tabs in the tab group (i.e. the last tab is removed from the group, which closes the group)? there might be other issues here but we should either remove the saved tab group when there are no tabs (an invalid state for a group) or keep the last tab and just consider it a "group close" instead of removing the tab.

Comment 18 by sheriffbot on Wed, Mar 16, 2022, 12:52 PM EDT

Labels: M-100 Target-100

Setting milestone and target because of medium severity.

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

Comment 19 by sheriffbot on Wed, Mar 16, 2022, 1:18 PM EDT

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 20 by sheriffbot on Wed, Mar 16, 2022, 2:23 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 21 by Git Watcher on Fri, Mar 18, 2022, 1:28 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f2d3c078ac66e0c535c357d8eeccc0d0fb795c4b

commit f2d3c078ac66e0c535c357d8eeccc0d0fb795c4b
Author: dljames <dljames@google.com>
Date: Fri Mar 18 17:27:41 2022

Fixes the use after free bug when creating multiple saved tab group buttons.

In short, we change OnTabGroupButtonPressed to take a const TabGroupID& so that when we use base::BindRepeating in CreateTabGroupButton the value is automagically copied in the call back. This prevents us from losing our saved tab group data and accessing garbage values.

More information for using const& can be found here:
https://chromium.googlesource.com/chromium/src.git/+/HEAD/docs/callback.md#binding-const-reference-parameters

~~Bug: 1305706~~
Change-Id: I62a9ba403416f964dc48013ea129c44084865ded
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3533522
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Darryl James <dljames@chromium.org>
Cr-Commit-Position: refs/heads/main@{#982768}

[modify]
https://crrev.com/f2d3c078ac66e0c535c357d8eeccc0d0fb795c4b/chrome/browser/ui/views/bookmarks/bookmark_bar_view.cc
[modify]
https://crrev.com/f2d3c078ac66e0c535c357d8eeccc0d0fb795c4b/chrome/browser/ui/views/bookmarks/bookmark_bar_view.h

Comment 22 by dljames@google.com on Fri, Mar 18, 2022, 1:33 PM EDT

Status: Fixed (was: Assigned)

Comment 23 by sheriffbot on Fri, Mar 18, 2022, 1:41 PM EDT

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

Comment 24 by sheriffbot on Sat, Mar 19, 2022, 12:41 PM EDT

Labels: reward-topanel

Comment 25 by sheriffbot on Sat, Mar 19, 2022, 2:10 PM EDT

Labels: Merge-Request-101 Merge-Request-100

Requesting merge to beta M100 because latest trunk commit (982768) appears to be after beta branch point (972766).

This is sufficiently serious that it should be merged to dev. I can't currently determine details for that channel, so please

This is sufficiently serious that it should be merged to dev. I can't currently determine details for that channel, so please assess whether this is already merged.

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

Comment 26 by sheriffbot on Mon, Mar 21, 2022, 2:50 PM EDT

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 27 by sheriffbot on Mon, Mar 21, 2022, 3:03 PM EDT

Labels: -Merge-Request-101 Hotlist-Merge-Approved Merge-Approved-101

Merge approved: your change passed merge requirements and is auto-approved for M101. Please go ahead and merge the CL to branch 4951 (refs/branch-heads/4951) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: None (Android), None (iOS), None (ChromeOS), None (Desktop)

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

Comment 28 by Git Watcher on Mon, Mar 21, 2022, 8:22 PM EDT

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/32b13d19412a9ed44d2c3892d1f75a394b84947e

commit 32b13d19412a9ed44d2c3892d1f75a394b84947e
Author: dljames <dljames@google.com>
Date: Tue Mar 22 00:21:31 2022

Fixes the use after free bug when creating multiple saved tab group buttons.

In short, we change OnTabGroupButtonPressed to take a const TabGroupID& so that when we use base::BindRepeating in CreateTabGroupButton the value is automagically copied in the call back. This prevents us from losing our saved tab group data and accessing garbage values.

More information for using const& can be found here:

More information for using const& can be found here:
https://chromium.googlesource.com/chromium/src.git/+/HEAD/docs/callback.md#binding-const-reference-parameters

(cherry picked from commit f2d3c078ac66e0c535c357d8eeccc0d0fb795c4b)

~~Bug: 1305706~~
Change-Id: I62a9ba403416f964dc48013ea129c44084865ded
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3533522
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Darryl James <dljames@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#982768}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3540921
Auto-Submit: Darryl James <dljames@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4951@{#29}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/32b13d19412a9ed44d2c3892d1f75a394b84947e/chrome/browser/ui/views/bookmarks/bookmark_bar_view.h
[modify]
https://crrev.com/32b13d19412a9ed44d2c3892d1f75a394b84947e/chrome/browser/ui/views/bookmarks/bookmark_bar_view.cc

Comment 29 by amyressler@chromium.org on Mon, Apr 4, 2022, 6:08 PM EDT

Labels: -Merge-Review-100 Merge-Approved-100

M100 merge approved, please merge to branch 4896 at your earliest convenience so this fix can be included in the next M100 stable refresh

Comment 30 by dlja...@chromium.org on Tue, Apr 5, 2022, 5:56 PM EDT

Labels: -Merge-Approved-100

No merge needed, feature was not implemented until m101 dropping merge to m100.

Comment 31 by amyressler@google.com on Fri, Apr 15, 2022, 1:09 PM EDT

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 32 by amyressler@chromium.org on Fri, Apr 15, 2022, 1:26 PM EDT

Hello, raven, and thank you for this report. Due to the highly significant amount of user interaction required to trigger this issue, the VRP Panel has decided to award you $2,000 for this report. Thank you for your efforts and reporting this issue to us.

Comment 33 by amyressler@google.com on Fri, Apr 15, 2022, 9:51 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 34 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:04 PM EDT

Labels: Release-0-M101

Comment 35 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT

Labels: CVE-2022-1491 CVE_description-missing

Comment 36 by sheriffbot on Sat, Jun 25, 2022, 1:31 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

Comment 37 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 38 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing