Starred by 2 users

Owner:	tbergquist@chromium.org
CC:	adetaylor@chromium.org pbomm...@chromium.org connily@chromium.org
Status:	Fixed *(Closed)*
Components:	----
Modified:	Jun 18, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
CVE_description-submitted
M-89
Target-89
LTS-Security-86
LTS-Security-NotApplicable-86
merge-merged-4389
merge-merged-89
Release-2-M89
CVE-2021-21192

Issue 1181387: Security: container-overflow in TabGroups

Reported by abalq...@microsoft.com on Tue, Feb 23, 2021, 3:06 PM EST

Code

VULNERABILITY DETAILS
Similar to ~~bug 1173093~~, but it seems that fix wasn't enough and we are still hitting container overflows in some instances.

VERSION
Chrome Version: 90.0.4427.0 (Developer Build) (64-bit)
Operating System: Windows 10 Pro

REPRODUCTION CASE
1. Host attached 'taber.html'
2. Run: ./chrome --user-data-dir=C:\asan\tabgroups --no-first-run --disable-popup-blocking http://localhost/taber.html?l "about:blank"
3. Hold shift and select all the about:blank tabs
4. Right click and create a tab group
5. Start dragging and dropping the group out of the main window and into a new window, repeat.

Crash should occur. See attached video for demo.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: Browser
Crash State: See attached asan log

CREDIT INFORMATION
Reporter credit: Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research

taber.html
477 bytes View Download

tabgroupsasan.txt
21.1 KB View Download

tabgroupcrash.mp4
1.2 MB View Download

Comment 1 by metzman@chromium.org on Wed, Feb 24, 2021, 11:12 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: connily@chromium.org
Labels: Security_Impact-Head Security_Severity-High OS-Windows Pri-1
Components: UI>Browser>TabStrip

I was able to reproduce this on Windows but not on Linux. I think it might be Windows only.
Although this requires user interaction that I don't think is super common I'll label it high severity like https://bugs.chromium.org/p/chromium/issues/detail?id=1173903
connily@ could you look into this?

Comment 2 by sheriffbot on Wed, Feb 24, 2021, 12:52 PM EST Project Member

Labels: M-90 Target-90

Setting milestone and target because of Security_Impact=Head and high severity.

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

Comment 3 by sheriffbot on Wed, Feb 24, 2021, 1:17 PM EST Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 4 by connily@chromium.org on Wed, Feb 24, 2021, 2:44 PM EST Project Member

Cc: tbergquist@chromium.org

Comment 5 by connily@chromium.org on Wed, Feb 24, 2021, 3:05 PM EST Project Member

Owner: tbergquist@chromium.org
Cc: -tbergquist@chromium.org connily@chromium.org

I was able to reproduce (though it's finicky because of the random timeouts), and I'll continue to help test, but Taylor is kindly going to help fix.

Comment 6 by tbergquist@chromium.org on Wed, Feb 24, 2021, 6:14 PM EST Project Member

Status: Started (was: Assigned)

Looks like there are just other cases in RevertDragAt where it can lose track of reverted tabs, and then try to update their group membership. I didn't go through it carefully enough the first time around, and missed some.

Comment 7 by bugdroid on Thu, Feb 25, 2021, 4:40 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/baed629809830c10b3d59ab88eb8fb7dbe7968c2

commit baed629809830c10b3d59ab88eb8fb7dbe7968c2
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Thu Feb 25 21:39:14 2021

Fix remaining instances of RevertDragAt losing track of tabs.

~~Bug: 1181287~~
Change-Id: I139383118a4b2059da1e28a90e467ebbe7fe139e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2719135
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Commit-Position: refs/heads/master@{#857850}

[modify] https://crrev.com/baed629809830c10b3d59ab88eb8fb7dbe7968c2/chrome/browser/ui/views/tabs/tab_drag_controller.cc

Comment 8 by tbergquist@chromium.org on Thu, Feb 25, 2021, 6:31 PM EST Project Member

Status: Fixed (was: Started)
Labels: Security_Impact-Stable

Fixed! Adding the appropriate security label since this crash should be able to occur on stable.

Comment 9 by sheriffbot on Fri, Feb 26, 2021, 12:21 PM EST Project Member

Labels: -security_impact-head

Comment 10 by adetaylor@google.com on Fri, Feb 26, 2021, 1:19 PM EST Project Member

Labels: -ReleaseBlock-Stable -M-90 -Target-90 M-89 Target-89 Merge-Request-89

Removing RBS due to #c8 and adjusting M, etc. Sheriffbot would add a merge request tomorrow so I'll short cut that.

Comment 11 by sheriffbot on Fri, Feb 26, 2021, 1:24 PM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: We are only 3 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), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 12 by sheriffbot on Fri, Feb 26, 2021, 1:55 PM EST Project Member

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

Comment 13 by pbommana@google.com on Fri, Feb 26, 2021, 2:23 PM EST Project Member

Cc: adetaylor@chromium.org pbomm...@chromium.org

+Adetaylor(Security TPM) for Merge Decision.

Comment 14 by tbergquist@chromium.org on Fri, Feb 26, 2021, 3:32 PM EST Project Member

1. Yes
2. https://chromium-review.googlesource.com/c/chromium/src/+/2719135
3. Not on ToT, but connily@ tested the patch. Requested, could you give it a test to verify the fix?
4. The impact goes quite a ways back, but it depends on https://chromium-review.googlesource.com/c/chromium/src/+/2682744 and would need to be merged on top of that CL so it doesn't merge conflict
5. They fix a crash
6. No
7. N/A

Comment 15 by tbergquist@chromium.org on Fri, Feb 26, 2021, 3:33 PM EST Project Member

Went ahead and posted a cherry-pick CL to 4389 here: https://chromium-review.googlesource.com/c/chromium/src/+/2724071

Comment 16 by adetaylor@chromium.org on Fri, Feb 26, 2021, 7:35 PM EST Project Member

Thanks, I'll approve M89 merges in a few days once the initial M89 release has been successfully made.

Comment 17 by adetaylor@google.com on Wed, Mar 10, 2021, 5:24 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389, unless any stability problems have shown up here since. Please go ahead and merge.

Comment 18 by Git Watcher on Thu, Mar 11, 2021, 3:11 PM EST Project Member

Labels: -merge-approved-89 merge-merged-4389 merge-merged-89

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ce80a25b427aa9c7f0f26b9d8452d7172f59a9b4

commit ce80a25b427aa9c7f0f26b9d8452d7172f59a9b4
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Thu Mar 11 20:10:03 2021

Fix remaining instances of RevertDragAt losing track of tabs.

(cherry picked from commit baed629809830c10b3d59ab88eb8fb7dbe7968c2)

~~Bug: 1191387~~
Change-Id: I139383118a4b2059da1e28a90e467ebbe7fe139e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2719135
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#857850}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2724071
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4389@{#1529}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/ce80a25b427aa9c7f0f26b9d8452d7172f59a9b4/chrome/browser/ui/views/tabs/tab_drag_controller.cc

Comment 19 by adetaylor@google.com on Thu, Mar 11, 2021, 6:17 PM EST Project Member

Labels: Release-2-M89

Comment 20 by adetaylor@google.com on Thu, Mar 11, 2021, 6:20 PM EST Project Member

Labels: CVE-2021-21192 CVE_description-missing

Comment 21 by janag...@google.com on Mon, Mar 15, 2021, 7:04 AM EDT Project Member

Labels: LTS-Security-NotApplicable-86

Comment 22 by amyressler@google.com on Tue, Mar 16, 2021, 10:13 AM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 23 by asumaneev@google.com on Thu, Apr 22, 2021, 10:48 AM EDT Project Member

Labels: LTS-Security-86

Comment 24 by sheriffbot on Fri, Jun 18, 2021, 1:51 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