

[chromium](#) ▾[New issue](#)[Open issues](#) ▾[Sign in](#)

☆ Starred by 4 users

Owner:dpenning@chromium.org**CC:**tbergquist@chromium.orgdpenning@chromium.org connily@chromium.orgamyressler@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:[Linux](#)**Pri:**

1

Type:[Bug-Security](#)

[Security_Severity-Medium](#)
[allpublic](#)
[reward-inprocess](#)
[Via-Wizard-Security](#)
[CVE_description-submitted](#)
[Target-97](#)
[external_security_report](#)
[M-98](#)
[reward-7000](#)
[Target-98](#)
[FoundIn-94](#)
[Security_Impact-Extended](#)
[Release-0-M100](#)
[CVE-2022-1136](#)
[TopChrome](#)

Issue 1280205: Security: Heap-use-after-free in TabStrip::OnGroupCreated

Reported by merc...@gmail.com on Wed, Dec 15, 2021, 5:53 AM EST

[↔](#) [Code](#)

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.81 Safari/537.36

Steps to reproduce the problem:

1. download asan-linux-release-951397.zip and unzip
2. start a server at the folder of poc.html : ``python -m SimpleHTTPServer 8605``
3. install the extension and allow website's popup
4. ``./chrome``, click the group header button (don't release). When you see the popup tab is opened, drag the tabgroup away, this will create two tabgroup with the same GroupId
5. drag the tabgroup back

What is the expected behavior?

What went wrong?

If we have two tabgroups with the same id and drag to merge them, old TabGroupViews will be freed in function

``TabStrip::OnGroupCreated`` [1] by assigning a new `unique_ptr` to ``group_views_[group]``.

and this old TabGroupViews will be used again in ``TabStripLayoutHelper::SlotsCollapsedTab`` [2], which is stored in ``slots_``.

[1]

https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/views/tabs/tab_strip.cc;l=1245;drc=0e45c020c43b1a9f6d2870ff7f92b30a2f03a458;bpv=0;bpt=0

[2]

https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/views/tabs/tab_strip_layout_helper.cc;l=443;drc=0e45c020c43b1a9f6d2870ff7f92b30a2f03a458;bpv=0;bpt=0

Did this work before? N/A

Chrome version: 94.0.4606.81 Channel: n/a

OS Version:

asan.txt

22.4 KB [View](#) [Download](#)

poc.html

150 bytes [View](#) [Download](#)

background.js

547 bytes [View](#) [Download](#)

manifest.json

210 bytes [View](#) [Download](#)

video.webm

6.0 MB [View](#) [Download](#)

0:00 / 0:17

[Comment 1](#) by [sheriffbot](#) on Wed, Dec 15, 2021, 5:54 AM EST

Labels: external_security_report

[Comment 2](#) by [merc....@gmail.com](#) on Wed, Dec 15, 2021, 5:56 AM EST

update the background.js

background.js

367 bytes [View](#) [Download](#)

[Comment 3](#) by [mea...@chromium.org](#) on Wed, Dec 15, 2021, 10:36 AM EST

Status: Assigned (was: Unconfirmed)

Owner: dpenning@chromium.org

Labels: Security_Severity-Medium FoundIn-94

Components: UI>Browser>TopChrome>TabStrip>TabGroups

Thanks for the report. I'm labeling this as medium severity: Despite being a bug in the UI, it needs an extension and a specific user gesture sequence to trigger, both of which are mitigating circumstances.

dpenning: Can I assign this to you since you are also looking at [bug-1270539](#)? Thanks.

[Comment 4](#) by [sheriffbot](#) on Wed, Dec 15, 2021, 10:38 AM EST

Labels: Security_Impact-Extended

[Comment 5](#) by [merc....@gmail.com](#) on Wed, Dec 15, 2021, 8:58 PM EST

Re Commnet 3:

Actually you can trigger this without extension, see video1.

video1.webm

547 KB [View](#) [Download](#)

0:00 / 0:17

[Comment 6](#) by [merc....@gmail.com](#) on Wed, Dec 15, 2021, 9:02 PM EST

1. start a server at the folder of poc.html : ``python -m SimpleHTTPServer 8605``
2. open chrome with ``./chrome http://127.0.0.1:8605/poc.html about:blank``
3. add the first tab to a group, and do the same steps in [comment 1](#)

[Comment 7](#) by [sheriffbot](#) on Thu, Dec 16, 2021, 12:52 PM EST

Labels: Target-97 M-97

Setting milestone and target because of medium severity.

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

[Comment 8](#) by [sheriffbot](#) on Thu, Dec 16, 2021, 1:18 PM EST

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 9](#) by [sheriffbot](#) on Wed, Dec 29, 2021, 12:21 PM EST

dpenning: 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 10](#) Deleted

[Comment 11](#) by [sheriffbot](#) on Tue, Jan 18, 2022, 12:21 PM EST

dpenning: 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 12](#) by [merc....@gmail.com](#) on Tue, Jan 18, 2022, 8:47 PM EST

any updates?

[Comment 13](#) by [dpenning@chromium.org](#) on Mon, Jan 24, 2022, 2:17 PM EST

<https://chromium-review.googlesource.com/c/chromium/src/+3404696> is out for review which fixes this behavior.

[Comment 14](#) by [dpenning@chromium.org](#) on Mon, Jan 24, 2022, 2:19 PM EST

Cc: [tbergquist@chromium.org](#) [dpenning@chromium.org](#) [connily@chromium.org](#) [amyressler@chromium.org](#)
~~Issue 1281079~~ has been merged into this issue.

[Comment 15](#) by [dpenning@chromium.org](#) on Mon, Jan 24, 2022, 2:19 PM EST

~~Issue 1282544~~ has been merged into this issue.

[Comment 16](#) by [sheriffbot](#) on Wed, Feb 2, 2022, 12:21 PM EST

Labels: -M-97 M-98 Target-98

[Comment 17](#) by [Git Watcher](#) on Thu, Feb 17, 2022, 12:16 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+d90543a244cfcf5d267a720ed86a37f5edd5835>

commit [d90543a244cfcf5d267a720ed86a37f5edd5835](#)

Author: David Pennington <[dpenning@chromium.org](#)>

Date: Thu Feb 17 17:15:45 2022

End TabDrag sessions before adding a new Tab to the TabStripModel

For multiple cases of TabGroupHeader dragging, when the tab strip model is changed to have a new tab in the group, the context doesn't currently pick it up. Because of this, the drag session needs to be ended before the tab can enter into the TabStripModel. This is because it picks the index for insertion based on where the group currently is, which may not be the intended destination for the tab when the drag is in a certain state.

In order to allow for this, a new signal is created for Observers of the TabStripModel OnTabWillBeAdded which is called before any mutation

tabStripModel On tabStripAdded which is called before any mutation occurs. This allows the drag code to cancel or complete its drag session before the new tab decides where it wants to go.

Bug-1280205

Change-Id: Id1e7d752ea1253695bf2f7a229e637415f8523c2

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+/3404696>

Reviewed-by: Connie Wan <connily@chromium.org>

Commit-Queue: David Pennington <dpenning@chromium.org>

Cr-Commit-Position: refs/heads/main@{#972499}

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/views/tabs/tab_drag_controller.h

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/views/tabs/browser_tab_strip_controller.h

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/tabs/tab_strip_model_observer.cc

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/tabs/tab_strip_model_observer.h

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/views/tabs/browser_tab_strip_controller.cc

[modify] https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/tabs/tab_strip_model.cc

[modify]

https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/views/tabs/tab_drag_controller.cc

[modify] https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/tabs/tab_strip_model.h

[modify] https://crrev.com/d90543a244cffcf5d267a720ed86a37f5edd5835/chrome/browser/ui/views/tabs/tab_strip_types.h

Comment 18 by merc....@gmail.com on Tue, Feb 22, 2022, 3:03 AM EST

Since this uaf can be triggered without extension, can we label it as severity-High and mark it as fixed?

Comment 19 by merc....@gmail.com on Tue, Mar 1, 2022, 1:54 AM EST

any updates?

Comment 20 by dpenning@chromium.org on Tue, Mar 1, 2022, 1:09 PM EST

Status: Fixed (was: Assigned)

Marking as fixed. Tested that this issue is fixed on canary along with the merged issues.

Comment 21 by [sheriffbot](#) on Tue, Mar 1, 2022, 1:41 PM EST

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

Comment 22 by [sheriffbot](#) on Wed, Mar 2, 2022, 12:41 PM EST

Labels: reward-topanel

Comment 23 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 PM EST

Labels: -reward-topanel reward-unpaid reward-7000

*** 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 24](#) by amyressler@chromium.org on Thu, Mar 10, 2022, 11:18 PM EST

Congratulations, the VRP Panel has decided to award you \$7,000 for this report. While we greatly appreciate your efforts, we feel it is important to note that issues are heavily or solely reliant on user interaction are likely receive reduced reward amounts in the future as of our rule/policy changes in this regard [1]. Thank you again for your efforts and reporting this issue to us.

[1] <https://g.co/chrome/vrp>

[Comment 25](#) by amyressler@google.com on Fri, Mar 11, 2022, 3:00 PM EST

Labels: -reward-unpaid reward-inprocess

[Comment 26](#) by amyressler@chromium.org on Mon, Mar 28, 2022, 6:14 PM EDT

Labels: Release-0-M100

[Comment 27](#) by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT

Labels: CVE-2022-1136 CVE_description-missing

[Comment 28](#) by [sheriffbot](#) on Wed, Jun 8, 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 29](#) by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

[Comment 30](#) by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)