☆ Starred by 1 user

| | |
|---|---|
| **Owner:** | tbergquist@chromium.org |
| **CC:** | adetaylor@chromium.org<br>janag...@google.com<br>connily@chromium.org<br>adetaylor@google.com |
| **Status:** | Fixed *(Closed)* |
| **Components:** | ---- |
| **Modified:** | May 14, 2021 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Windows, Chrome, Mac, Fuchsia |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Security_Impact-Stable
Security_Severity-High
ReleaseBlock-Stable
allpublic
CVE_description-submitted
M-90
Target-90
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
merge-merged-4324
merge-merged-88
merge-merged-89
Release-3-M88
CVE-2021-21154

### Issue 1173269: Security: heap-buffer-overflow in TabStripModel

Reported by abalq...@microsoft.com on Mon, Feb 1, 2021, 6:55 PM EST

Code

**VULNERABILITY DETAILS**
**Please provide a brief explanation of the security issue.**

**VERSION**
Chrome Version: 90.0.4406.0 (Developer Build) (64-bit)
Operating System: Windows 10 OS Version 1909 (Build 18363.1316)

**REPRODUCTION CASE**

1. Host attached PoC and run:

```
./chrome.exe --user-data-dir=C:\asan\qtabs --no-first-run --disable-popup-blocking http://localhost/tabs.html
```

2. Once you see 3 tabs, hodl down shift and click on the main tab (to the left) in order to select all tabs

3. Start dragging the group of tabs and crash will occur.

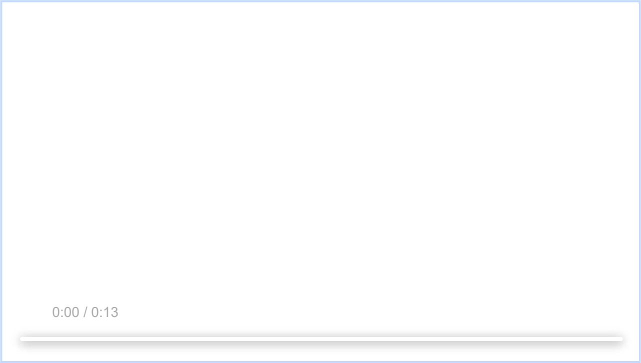
Only tested on Windows 10, see attached video for demo of steps.

**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

**tabsasan.txt**
22.1 KB View Download

**tabs.mp4**
1.5 MB View Download



**tabs.html**
874 bytes View Download

Comment 1 by tsepez@chromium.org on Tue, Feb 2, 2021, 1:04 PM EST Project Member

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

connily - related to the work done in
https://chromium-review.googlesource.com/c/chromium/src/+/2020908 ?

Setting sev-high (would be critical for overflow in browser but mitigated by the user-interaction required).
Per the linked CL, I believe this only affects head, but let us know if you believe this goes further back.
Likely to apply to all desktop platforms.

Thanks!

Comment 2 by connily@chromium.org on Tue, Feb 2, 2021, 1:14 PM EST Project Member

I don't think this is related to the CL linked in comment #1, but the repro steps look very similar to https://bugs.chromium.org/p/chromium/issues/detail?id=1151799
However, that bug should be fixed at head. I'll try the repro again, as well as the one in this bug.

Comment 3 by sheriffbot on Tue, Feb 2, 2021, 1:21 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 sheriffbot on Wed, Feb 3, 2021, 12:54 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 5 by connily@chromium.org on Wed, Feb 3, 2021, 2:23 PM EST Project Member

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

+Taylor has kindly agreed to help take a look here, as I'm not sure I can address these in a reasonable timeframe.

Taylor, these all look pretty similar to each other and to https://bugs.chromium.org/p/chromium/issues/detail?id=1151799, but with slightly different repros and stack traces.
Please feel free to grab some time with me to go over them, or just chat asynchronously.

Thank you!!

Comment 6 by connily@chromium.org on Thu, Feb 4, 2021, 12:48 PM EST Project Member

Fix for this bug should be in https://chromium-review.googlesource.com/c/chromium/src/+/2673973 (we had the wrong bug attached to the CL).

Comment 7 by tbergquist@chromium.org on Thu, Feb 4, 2021, 7:44 PM EST Project Member

**Status:** Fixed (was: Assigned)

Requester, can I ask you to verify the issue is resolved with https://chromium-review.googlesource.com/c/chromium/src/+/2673973 ?

Comment 8 by abalq...@microsoft.com on Fri, Feb 5, 2021, 9:49 AM EST

LGTM

Comment 9 by sheriffbot on Fri, Feb 5, 2021, 1:57 PM EST Project Member

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

Comment 10 by tsepez@chromium.org on Tue, Feb 9, 2021, 6:50 PM EST Project Member

**Labels:** -Security_Impact-Head Security_Impact-Stable

Comment 11 by adetaylor@google.com on Tue, Feb 9, 2021, 6:50 PM EST Project Member

**Labels:** Merge-Request-88 Merge-Approved-89

After discussion with Taylor we consider that this impacts Stable. Applying suitable merge approval to M89 (branch 4389) and a request for M88 merge to be considered later.

Comment 12 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:23 PM EST Project Member

**Labels:** -Merge-Request-88 Merge-Approved-88

Approving merge also to M88, branch 4324.

Comment 13 by bugdroid on Wed, Feb 10, 2021, 6:17 PM EST Project Member

**Labels:** -merge-approved-88 merge-merged-4324 merge-merged-88

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/732093c0526299a24ed4e3fa14f8000ca2f7c39d

commit 732093c0526299a24ed4e3fa14f8000ca2f7c39d
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Wed Feb 10 23:16:50 2021

Fix crash when reverting a drag if the source tabstrip changed during the drag.

(cherry picked from commit 88be7f3b2b017c2f7b904db368391182e296b11e)

(cherry picked from commit 13d703e9b199942e1241ccf395a8e51619b01597)

~~Bug: 1173269~~
Change-Id: Ic6a6faa554c0ef1d6082e98a04a58ccfb5c5cac5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2673973
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#850424}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2685424
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Connie Wan <connily@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4389@{#898}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688310
Cr-Commit-Position: refs/branch-heads/4324@{#2164}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/732093c0526299a24ed4e3fa14f8000ca2f7c39d/chrome/browser/ui/tabs/tab_strip_model.h
[modify] https://crrev.com/732093c0526299a24ed4e3fa14f8000ca2f7c39d/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 14 by adetaylor@google.com on Fri, Feb 12, 2021, 7:35 PM EST Project Member

**Labels:** Release-3-M88

Comment 15 by sheriffbot on Mon, Feb 15, 2021, 12:14 PM EST Project Member

**Cc:** adetaylor@google.com adetaylor@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 16 by janag...@google.com on Mon, Feb 15, 2021, 12:15 PM EST Project Member

**Cc:** janag...@google.com
**Labels:** LTS-Security-86 Merge-Request-86-LTS

Comment 17 by gianluca@google.com on Tue, Feb 16, 2021, 3:43 AM EST Project Member

**Labels:** Merge-Approved-86-LTS

Comment 18 by bugdroid on Wed, Feb 17, 2021, 6:00 AM EST Project Member

**Labels:** merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0c76a72c4db232b57e7367a6287a53ca6e4904b2

commit 0c76a72c4db232b57e7367a6287a53ca6e4904b2
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Wed Feb 17 10:59:09 2021

Fix crash when reverting a drag if the source tabstrip changed during the drag.

(cherry picked from commit 88be7f3b2b017c2f7b904db368391182e296b11e)

(cherry picked from commit 13d703e9b199942e1241ccf395a8e51619b01597)

(cherry picked from commit 732093c0526299a24ed4e3fa14f8000ca2f7c39d)

~~Bug: 1173269~~
Change-Id: Ic6a6faa554c0ef1d6082e98a04a58ccfb5c5cac5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2673973
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Cr-Original-Original-Original-Commit-Position: refs/heads/master@{#850424}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2685424
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Connie Wan <connily@chromium.org>
Cr-Original-Original-Commit-Position: refs/branch-heads/4389@{#898}
Cr-Original-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688310
Cr-Original-Commit-Position: refs/branch-heads/4324@{#2164}
Cr-Original-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2693623
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Jana Grill <janagrill@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1543}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/0c76a72c4db232b57e7367a6287a53ca6e4904b2/chrome/browser/ui/tabs/tab_strip_model.h
[modify] https://crrev.com/0c76a72c4db232b57e7367a6287a53ca6e4904b2/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 19 by janag...@google.com on Wed, Feb 17, 2021, 7:58 AM EST Project Member

**Labels:** -Merge-Request-86-LTS -Merge-Approved-86-LTS LTR-Merged-86

Comment 20 by pbommana@google.com on Thu, Feb 18, 2021, 1:00 PM EST Project Member

The change was merged to M89 as part of https://chromium-review.googlesource.com/c/chromium/src/+/2685424.

Taylor pinged me offline and informed that he got the bug_id wrong i.e., 1173629 instead of 1173269.

@adetaylor want to check if this exposed something, Since 1173629 is a public bug?

Comment 21 by adetaylor@chromium.org on Thu, Feb 18, 2021, 1:03 PM EST Project Member

**Labels:** -Merge-Approved-89 merge-merged-89

No worries about the exposure. CLs are publicly visible in gerrit anyway. Thanks for checking though.

Comment 22 by amyressler@google.com on Mon, Feb 22, 2021, 4:31 PM EST Project Member

**Labels:** CVE-2021-21154 CVE_description-missing

Comment 23 by amyressler@google.com on Mon, Feb 22, 2021, 4:33 PM EST Project Member

**Labels:** -CVE_description-missing CVE_description-submitted

Comment 24 by sheriffbot on Fri, May 14, 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