Starred by 4 users

Owner:	tbergquist@chromium.org
CC:	adetaylor@chromium.org pbomm...@chromium.org connily@chromium.org rsleevi@chromium.org dfried@chromium.org
Status:	Verified *(Closed)*
Components:	----
Modified:	May 26, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
Target-88
M-88
Merge-Rejected-88
LTS-Security-86
LTS-Security-NotApplicable-86
Release-0-M89
external_security_report
merge-merged-4389
merge-merged-89
CVE-2021-21159

Issue 1171049: Security: container-overflow in TabStrip::SetSelection

Reported by chrom...@gmail.com on Tue, Jan 26, 2021, 9:37 PM EST

Code

VERSION
Chrome Version: 90.0.4399.0 (Official Build) canary (x86_64)
Operating System: MacOS

REPRODUCTION CASE

Similar to ~~issue 1138911~~

1. Run chrome with "about:blank" "http://localhost:8000/poc.html" "about:blank"
2. In the second tab click on the button then to drag the third tab "about:blank" out of the current tab strip slowly >> crash

```
==5135==ERROR: AddressSanitizer: container-overflow on address 0x60800020d438 at pc 0x000123203fb9 bp 0x7fff5a5c91f0 sp 0x7fff5a5c91e8
READ of size 8 at 0x60800020d438 thread T0
    #0 0x123203fb8 in TabStrip::SetSelection(ui::ListSelectionModel const&) view_model.h:81
    #1 0x123166f4a in BrowserTabStripController::OnTabStripModelChanged(TabStripModel*, TabStripModelChange const&, TabStripSelectionChange const&)
browser_tab_strip_controller.cc:689
    #2 0x122673a0b in TabStripModel::SetSelection(ui::ListSelectionModel, TabStripModelObserver::ChangeReason, bool) tab_strip_model.cc:1884
    #3 0x12267ba92 in TabStripModel::SetSelectionFromModel(ui::ListSelectionModel) tab_strip_model.cc:915
    #4 0x1231ba9b2 in TabDragController::RestoreInitialSelection() tab_drag_controller.cc:1673
    #5 0x1231b641c in TabDragController::Detach(TabDragController::ReleaseCapture) tab_drag_controller.cc:1322
    #6 0x1231b530d in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) tab_drag_controller.cc:1373
    #7 0x1231b30bf in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) tab_drag_controller.cc:865
    #8 0x1231b03f4 in TabDragController::ContinueDragging(gfx::Point const&) tab_drag_controller.cc:831
    #9 0x1231a908a in TabDragController::Drag(gfx::Point const&) tab_drag_controller.cc:604
    #10 0x123209f97 in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) tab_strip.cc:462
    #11 0x12321690b in TabStrip::OnMouseDragged(ui::MouseEvent const&) tab_strip.cc:3654
    #12 0x12212480d in views::View::ProcessMouseDragged(ui::MouseEvent*) view.cc:2976
    #13 0x119ba5e8f in ui::EventHandler::OnEvent(ui::Event*) event_handler.cc
    #14 0x119ba4279 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
    #15 0x119ba3a54 in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
    #16 0x119ba3780 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:56
    #17 0x1221576fa in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) root_view.cc:452
    #18 0x12217296a in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1326
    #19 0x11e056b3c in -[BridgedContentView mouseEvent:] bridged_content_view.mm:586
    #20 0x11e053dd7 in -[BridgedContentView processCapturedMouseEvent:] bridged_content_view.mm:308
    #21 0x11e06242b in ___ZN12remote_cocoa17CocoaMouseCapture14ActiveEventTap4InitEv_block_invoke mouse_capture.mm:91
    #22 0x7fff95ecb7f9 in _NSSendEventToObservers+0x173 (AppKit:x86_64+0x1c77f9)
    #23 0x7fff964c423e in -[NSApplication(NSEvent) sendEvent:]+0x36 (AppKit:x86_64+0x7c023e)
    #24 0x117751474 in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:327
    #25 0x11653e1b9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xb4221b9)
    #26 0x1177504c6 in -[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:311
    #27 0x7fff95d3f3d6 in -[NSApplication run]+0x3e9 (AppKit:x86_64+0x3b3d6)
    #28 0x1165525da in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*) message_pump_mac.mm:691
    #29 0x11654e1b8 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*) message_pump_mac.mm:149
```

```
    #30 0x11646281b in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
thread_controller_with_message_pump_impl.cc:460
    #31 0x1163a888b in base::RunLoop::Run() run_loop.cc:131
    #32 0x116a74261 in ChromeBrowserMainParts::MainMessageLoopRun(int*) chrome_browser_main.cc:1736
    #33 0x10f94bef9 in content::BrowserMainLoop::RunMainMessageLoopParts() browser_main_loop.cc:970
    #34 0x10f9514c1 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:150
    #35 0x10f94376c in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:47
    #36 0x116185175 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content_main_runner_impl.cc:555
    #37 0x1161844c3 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:926
    #38 0x11618125b in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content_main.cc:372
    #39 0x11618191c in content::ContentMain(content::ContentMainParams const&) content_main.cc:398
    #40 0x10b121a35 in ChromeMain chrome_main.cc:141
    #41 0x105633eff in main chrome_exe_main_mac.cc:114
    #42 0x7fffade9f234 in start+0x0 (libdyld.dylib:x86_64+0x5234)

0x60800020d438 is located 24 bytes inside of 96-byte region [0x60800020d420,0x60800020d480)
allocated by thread T0 here:
    #0 0x105818d30  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x45d30)
    #1 0x1162a6387 in operator new(unsigned long) new.cpp:67
    #2 0x12214b6f6 in std::__1::vector<views::ViewModelBase::Entry, std::__1::allocator<views::ViewModelBase::Entry>
>::insert(std::__1::__wrap_iter<views::ViewModelBase::Entry const*>, views::ViewModelBase::Entry const&) __split_buffer:318
    #3 0x12214c032 in views::ViewModelBase::AddUnsafe(views::View*, int) view_model.cc:74
    #4 0x1231f8c82 in TabStrip::AddTabAt(int, TabRendererData, bool) tab_strip.cc:1271
    #5 0x123161e4d in BrowserTabStripController::AddTab(content::WebContents*, int, bool) browser_tab_strip_controller.cc:775
    #6 0x123166a40 in BrowserTabStripController::OnTabStripModelChanged(TabStripModel*, TabStripModelChange const&, TabStripSelectionChange const&)
browser_tab_strip_controller.cc:639
    #7 0x12266e30e in TabStripModel::InsertWebContentsAtImpl(int, std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, int,
base::Optional<tab_groups::TabGroupId>) tab_strip_model.cc:1726
    #8 0x12267c317 in TabStripModel::AddWebContents(std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, int,
ui::PageTransition, int, base::Optional<tab_groups::TabGroupId>) tab_strip_model.cc:986
    #9 0x1224bb48a in Navigate(NavigateParams*) browser_navigator.cc:715
    #10 0x122636642 in StartupBrowserCreatorImpl::OpenTabsInBrowser(Browser*, bool, std::__1::vector<StartupTab, std::__1::allocator<StartupTab> > const&)
startup_browser_creator_impl.cc:273
    #11 0x122638ddf in StartupBrowserCreatorImpl::RestoreOrCreateBrowser(std::__1::vector<StartupTab, std::__1::allocator<StartupTab> > const&,
StartupBrowserCreatorImpl::BrowserOpenBehavior, unsigned int, bool, bool) startup_browser_creator_impl.cc:519
    #12 0x122635682 in StartupBrowserCreatorImpl::DetermineURLsAndLaunch(bool, std::__1::vector<GURL, std::__1::allocator<GURL> > const&)
startup_browser_creator_impl.cc:383
    #13 0x122634c6a in StartupBrowserCreatorImpl::Launch(Profile*, std::__1::vector<GURL, std::__1::allocator<GURL> > const&, bool,
std::__1::unique_ptr<LaunchModeRecorder, std::__1::default_delete<LaunchModeRecorder> >) startup_browser_creator_impl.cc:186
    #14 0x122628448 in StartupBrowserCreator::LaunchBrowser(base::CommandLine const&, Profile*, base::FilePath const&, chrome::startup::IsProcessStartup,
chrome::startup::IsFirstRun, std::__1::unique_ptr<LaunchModeRecorder, std::__1::default_delete<LaunchModeRecorder> >) startup_browser_creator.cc:523
    #15 0x1226304cc in StartupBrowserCreator::ProcessLastOpenedProfiles(base::CommandLine const&, base::FilePath const&, chrome::startup::IsProcessStartup,
chrome::startup::IsFirstRun, Profile*, std::__1::vector<Profile*, std::__1::allocator<Profile*> > const&) startup_browser_creator.cc:1034
    #16 0x12262fc7a in StartupBrowserCreator::LaunchBrowserForLastProfiles(base::CommandLine const&, base::FilePath const&, bool, Profile*, std::__1::vector<Profile*,
std::__1::allocator<Profile*> > const&) startup_browser_creator.cc:984
    #17 0x1226278f5 in StartupBrowserCreator::ProcessCmdLineImpl(base::CommandLine const&, base::FilePath const&, bool, Profile*, std::__1::vector<Profile*,
std::__1::allocator<Profile*> > const&) startup_browser_creator.cc:922
    #18 0x122625b27 in StartupBrowserCreator::Start(base::CommandLine const&, base::FilePath const&, Profile*, std::__1::vector<Profile*, std::__1::allocator<Profile*> >
const&) startup_browser_creator.cc:475
    #19 0x116a71b98 in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome_browser_main.cc:1636
    #20 0x116a6f276 in ChromeBrowserMainParts::PreMainMessageLoopRun() chrome_browser_main.cc:1041
    #21 0x10f94bae2 in content::BrowserMainLoop::PreMainMessageLoopRun() browser_main_loop.cc:944
    #22 0x110ac0c3f in content::StartupTaskRunner::RunAllTasksNow() callback.h:101
    #23 0x10f94803c in content::BrowserMainLoop::CreateStartupTasks() browser_main_loop.cc:854
    #24 0x10f950adc in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) browser_main_runner_impl.cc:129
    #25 0x10f94371a in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:43
    #26 0x116185175 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content_main_runner_impl.cc:555
    #27 0x1161844c3 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:926
    #28 0x11618125b in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content_main.cc:372
    #29 0x11618191c in content::ContentMain(content::ContentMainParams const&) content_main.cc:398

HINT: if you don't care about these errors you may set ASAN_OPTIONS=detect_container_overflow=0.
If you suspect a false positive see also: https://github.com/google/sanitizers/wiki/AddressSanitizerContainerOverflow.
SUMMARY: AddressSanitizer: container-overflow view_model.h:81 in TabStrip::SetSelection(ui::ListSelectionModel const&)
Shadow bytes around the buggy address:
  0x1c1000041a30: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fa
  0x1c1000041a40: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fa
  0x1c1000041a50: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fa
  0x1c1000041a60: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c1000041a70: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 fa
=>0x1c1000041a80: fa fa fa fa 00 00 00[fc]fc fc fc fc fc fc fc fc
  0x1c1000041a90: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fa
  0x1c1000041aa0: fa fa fa fa 00 00 00 00 00 00 fc fc fc fc fc fc
  0x1c1000041ab0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c1000041ac0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c1000041ad0: fa fa fa fa 00 00 00 fc fc fc fc fc fc fc fc fc
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
```

[Deleted] **screen.mov**

poc.html
176 bytes View Download

Comment 1 by sheriffbot on Tue, Jan 26, 2021, 9:42 PM EST Project Member

Labels: external_security_report

Comment 2 by rsleevi@chromium.org on Wed, Jan 27, 2021, 5:51 PM EST Project Member

Labels: Needs-Feedback
Components: UI>Browser>TabStrip

Thanks for reporting this.

I'm unable to reproduce this issue, as the window.close() call in your trigger is blocked due to long-standing policies that prevent scripts from closing windows. Could you provide more details about your steps to reproduce?

Comment 3 by rsleevi@chromium.org on Wed, Jan 27, 2021, 6:03 PM EST Project Member

Cc: sky@chromium.org dfried@chromium.org

Comment 4 by chrom...@gmail.com on Wed, Jan 27, 2021, 6:15 PM EST

Okey, I have another way to repro.

1. Run chrome with "about:blank" "http://localhost:8000/poc.html" "about:blank"

2. In the second tab (http://localhost:8000/poc.html) click on the button then drag the third tab to the right and wait till http://localhost:8000/poc.html is closed then try to get it back to the left (next to the first tab).

screen.mov
3.6 MB View Download

Comment 5 by sheriffbot on Wed, Jan 27, 2021, 6:19 PM EST Project Member

Cc: rsleevi@chromium.org
Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 6 by rsleevi@chromium.org on Wed, Jan 27, 2021, 6:27 PM EST Project Member

Labels: Needs-Feedback

Sorry I wasn't clearer: Your trigger button does not close the window, because it's being blocked from doing so due to existing security policies (specifically, the attempt to close the window is blocked by this line:
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/frame/dom_window.cc;l=347;drc=e1facbdd9b6cfe6f5ec53f8b20e662c934e75045)

I wanted to make sure you're not running with any custom command-line flags or options here that would be useful to verify the repro.

Comment 7 by chrom...@gmail.com on Wed, Jan 27, 2021, 7:07 PM EST

I'm able to repro this in a fresh profile.

Can you attach a screen recording using Quicktime?

Comment 8 by sheriffbot on Wed, Jan 27, 2021, 7:11 PM EST Project Member

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 9 by rsleevi@chromium.org on Wed, Jan 27, 2021, 7:41 PM EST Project Member

No.

Comment 10 by chrom...@gmail.com on Wed, Jan 27, 2021, 7:47 PM EST

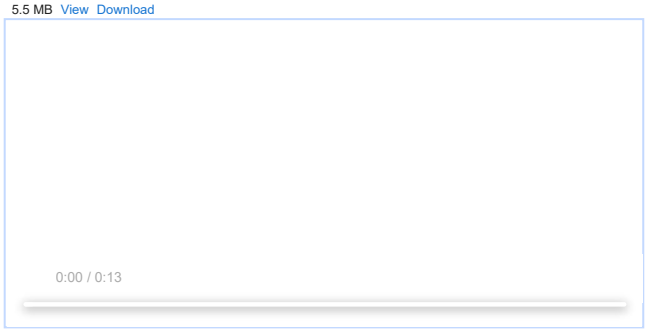
Note: window.close() requires that your tab has no history to close the window (won't work unless you have a fresh browsing session.)

Please chrome as:

$ out/asan/chrome --user-data-dir=/tmp/xxxx "about:blank" "http://localhost:8000/poc.html" "about:blank"

Comment 11 by chrom...@gmail.com on Wed, Jan 27, 2021, 7:58 PM EST

screen.mov
5.5 MB View Download



Comment 12 by rsleevi@chromium.org on Wed, Jan 27, 2021, 8:18 PM EST Project Member

Thanks for confirming there are added command-line flags! ;-) Indeed, I was attempting to better understand the launch scenario, precisely because of the line mentioned in Comment #6 provides several mitigations to prevent arbitrary window.close()ing

I'm not seeing this reproduce in 90.0.4401.0 (r847401), nor in 90.0.4399.0 (r 846616), on macOS or Linux, with an ASAN build, with file:// URLs or a local server, with dragging within the window or detaching.

Comment 13 by rsleevi@chromium.org on Wed, Jan 27, 2021, 8:18 PM EST Project Member

(To be clear, the Window does indeed close, but no ASAN errors)

Comment 14 by rsleevi@chromium.org on Wed, Jan 27, 2021, 8:22 PM EST Project Member

Labels: Security_Severity-High Security_Impact-Head Pri-1

Nevermind, it's clear that it's detach-after-close rather than release-after-close :)

Comment 15 by rsleevi@chromium.org on Wed, Jan 27, 2021, 8:59 PM EST Project Member

Labels: -Security_Impact-Head Security_Impact-Stable

Comment 16 by rsleevi@chromium.org on Wed, Jan 27, 2021, 9:05 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: sky@chromium.org
Cc: -sky@chromium.org

Sky: Could you help route this appropriately?

Comment 17 by sheriffbot on Thu, Jan 28, 2021, 12:45 PM EST Project Member

Labels: Target-88 M-88

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 18 by sky@chromium.org on Fri, Jan 29, 2021, 3:55 PM EST Project Member

Owner: tbergquist@chromium.org

tbergquist is likely the right person.

Comment 19 by rsleevi@chromium.org on Mon, Feb 1, 2021, 3:27 PM EST Project Member

Labels: OS-Linux OS-Windows

Comment 20 by chrom...@gmail.com on Wed, Feb 3, 2021, 10:53 PM EST

rsleevi@ Thanks for comment#14

Comment 21 by sheriffbot on Wed, Feb 10, 2021, 12:21 PM EST Project Member

tbergquist: 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 22 by tbergquist@chromium.org on Wed, Feb 10, 2021, 4:56 PM EST Project Member

Hey, I've fixed a number of similar bugs lately but this one somehow slipped under my radar. Could I ask you to please check if this still reproduces on the latest Canary?

Comment 23 by chrom...@gmail.com on Wed, Feb 10, 2021, 5:03 PM EST

Yes, I'm still able to repro this on Canary 90.0.4414.0.

Comment 24 by tbergquist@chromium.org on Wed, Feb 10, 2021, 7:27 PM EST Project Member

Cc: connily@chromium.org

Okay, I've posted a WIP candidate fix here: https://chromium-review.googlesource.com/c/chromium/src/+/2688619/
I can't test this (I only have a mac to work on) but CCing Connie who can. Meanwhile reviving my cloudtop in case I need more iteration than this.

Comment 25 by bugdroid on Thu, Feb 11, 2021, 5:49 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/248d3eb06950a4055afc8975fb801334fb8b2118

commit 248d3eb06950a4055afc8975fb801334fb8b2118
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Thu Feb 11 22:48:12 2021

Fix crash when detaching a drag after a tab closed.

~~Bug: 1171049~~
Change-Id: Ia47934714f4bb5376d1f8abbabbe0a3cd22422a3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688619
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Commit-Position: refs/heads/master@{#853260}

[modify] https://crrev.com/248d3eb06950a4055afc8975fb801334fb8b2118/chrome/browser/ui/views/tabs/tab_drag_controller.cc
[modify] https://crrev.com/248d3eb06950a4055afc8975fb801334fb8b2118/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 26 by chrom...@gmail.com on Mon, Feb 15, 2021, 10:49 AM EST

Fixed on Canary 90.0.4418.0. Thanks as ever!

Comment 27 by tbergquist@chromium.org on Tue, Feb 16, 2021, 4:59 PM EST Project Member

Status: Verified (was: Assigned)

:D

Comment 28 by sheriffbot on Wed, Feb 17, 2021, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 29 by sheriffbot on Wed, Feb 17, 2021, 1:57 PM EST Project Member

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

Comment 30 by sheriffbot on Wed, Feb 17, 2021, 2:18 PM EST Project Member

Labels: Merge-Request-89 Merge-Request-88

Requesting merge to stable M88 because latest trunk commit (853260) appears to be after stable branch point (827102).

Requesting merge to beta M89 because latest trunk commit (853260) appears to be after beta branch point (843830).

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

Comment 31 by sheriffbot on Wed, Feb 17, 2021, 2:22 PM EST Project Member

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

This bug requires manual review: We are only 12 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 32 by tbergquist@google.com on Wed, Feb 17, 2021, 5:17 PM EST Project Member

1) I'd want security's input on whether the merge is warranted. It's a lowish-complexity fix, mostly I'm unsure how critical of a security issue it is vs the bar for a later merge.
2) https://chromium-review.googlesource.com/c/chromium/src/+/2688619
3) Yes
4) It could go into 88, but it already has the label for that.
5) It fixes an exploitable bug
6) No
7) N/A

Comment 33 by pbommana@google.com on Thu, Feb 18, 2021, 1:38 PM EST Project Member

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

+Adetaylor@(Security TPM) for merge review

Comment 34 by adetaylor@chromium.org on Thu, Feb 18, 2021, 8:43 PM EST Project Member

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

Yes, please merge to M89, branch 4389.

There's unlikely to be another M88 release but I'll keep the Merge-Request-88 label until we're certain.

Comment 35 by bugdroid on Fri, Feb 19, 2021, 7:22 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3ad5c3e55c9353d7c60f4ad1424039c96d598cce

commit 3ad5c3e55c9353d7c60f4ad1424039c96d598cce
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Sat Feb 20 00:22:19 2021

Fix crash when detaching a drag after a tab closed.

(cherry picked from commit 248d3eb06950a4055afc8975fb801334fb8b2118)

~~Bug: 1171049~~
Change-Id: Ia47934714f4bb5376d1f8abbabbe0a3cd22422a3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688619
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#853260}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2708624
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4389@{#1229}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/3ad5c3e55c9353d7c60f4ad1424039c96d598cce/chrome/browser/ui/views/tabs/tab_drag_controller.cc
[modify] https://crrev.com/3ad5c3e55c9353d7c60f4ad1424039c96d598cce/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 36 by amyressler@google.com on Wed, Feb 24, 2021, 6:40 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 37 by amyressler@google.com on Wed, Feb 24, 2021, 7:05 PM EST Project Member

Congratulations, Khalil! The VRP Panel has decided to award you $10,000 for this report. Nice work!

Comment 38 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 39 by amyressler@google.com on Fri, Feb 26, 2021, 3:23 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 40 by adetaylor@google.com on Fri, Feb 26, 2021, 4:44 PM EST Project Member

Labels: -Merge-Request-88 Merge-Rejected-88

Not merging to M88 - no further releases planned.

Comment 41 by asumaneev@google.com on Mon, Mar 1, 2021, 4:48 PM EST Project Member

Labels: LTS-Security-86 LTS-Security-NotApplicable-86

Marking as not applicable for LTS since introducing code landed after M86 (same as ~~https://crbug.com/1163845~~).

Comment 42 by adetaylor@google.com on Mon, Mar 1, 2021, 7:26 PM EST Project Member

Labels: CVE-2021-21159 CVE_description-missing

Comment 43 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 44 by sheriffbot on Wed, May 26, 2021, 1:55 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