☆ Starred by 3 users

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

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
Target-88
M-88
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
merge-merged-4324
merge-merged-88
external_security_report
merge-merged-4389
merge-merged-89
Release-3-M88
CVE-2021-21155

Issue 1175500: Security: Heap-buffer-overflow in TabStripModel::GroupTab (Windows-only)

Reported by chrom...@gmail.com on Sat, Feb 6, 2021, 7:24 PM EST

Code

VERSION
Chrome Version: stable and canary 90.0.4411.0
Operating System: Windows 7

REPRODUCTION CASE
1. python -m SimpleHTTPServer
2. chrome.exe "http://localhost:8000/poc.html" "about:blank"
3. Add http://localhost:8000/poc.html to a new group.
4. Add about:blank tab to the group (http://localhost:8000/poc.html)
5. In http://localhost:8000/poc.html click on the button and hold the mouse over the grey point and keep dragging on

```
==5516==ERROR: AddressSanitizer: container-overflow on address 0x010741df3fe0 at pc 0x07fec22eeebd bp 0x00000084cbe0 sp 0x00000084cc28

READ of size 8 at 0x010741df3fe0 thread T0
   #0 0x7fec22eeebc in std::__1::unique_ptr<TabStripModel::WebContentsData,std::default_delete<TabStripModel::WebContentsData> >::ope
rator-> C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory:2602
   #1 0x7fec22eeebc in TabStripModel::GroupTab(int, class tab_groups::TabGroupId const &) C:\b\s\w\ir\cache\builder\src\chrome\browse
r\ui\tabs\tab_strip_model.cc:2187:54
   #2 0x7fec22ee484 in TabStripModel::UpdateGroupForDragRevert(int, class base::Optional<class tab_groups::TabGroupId>, class base::O
ptional<class tab_groups::TabGroupVisualData>) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_strip_model.cc:1101:5
   #3 0x7feca9ea57b in TabDragController::RevertDragAt(unsigned __int64) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs\t
ab_drag_controller.cc:1731:40
   #4 0x7feca9e830a in TabDragController::RevertDrag(void) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs\tab_drag_contro
ller.cc:1598:7
   #5 0x7feca9de6c6 in TabDragController::EndDragImpl(enum TabDragController::EndDragType) C:\b\s\w\ir\cache\builder\src\chrome\brows
er\ui\views\tabs\tab_drag_controller.cc:1528:11
   #6 0x7feca9d7346 in TabDragController::EndDrag(enum EndDragReason) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs\tab_
drag_controller.cc:646:3
   #7 0x7feca9dd438 in TabDragController::RunMoveLoop(class gfx::Vector2d const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\vi
ews\tabs\tab_drag_controller.cc:1453:5
   #8 0x7feca9e232f in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(class gfx::Point const &) C:\b\s\w\ir\cache\builder\src\
chrome\browser\ui\views\tabs\tab_drag_controller.cc:1390:3
   #9 0x7feca9e0038 in TabDragController::DragBrowserToNewTabStrip(class TabDragContext *, class gfx::Point const &) C:\b\s\w\ir\cach
e\builder\src\chrome\browser\ui\views\tabs\tab_drag_controller.cc:865:5
   #10 0x7feca9ddc28 in TabDragController::ContinueDragging(class gfx::Point const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui
\views\tabs\tab_drag_controller.cc:831:9
   #11 0x7feca9d8300 in TabDragController::Drag(class gfx::Point const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs\
tab_drag_controller.cc:604:7
   #12 0x7fec79aeb08 in TabStrip::TabDragContextImpl::ContinueDrag(class views::View *, class ui::LocatedEvent const &) C:\b\s\w\ir\c
ache\builder\src\chrome\browser\ui\views\tabs\tab_strip.cc:462:25
   #13 0x7fec79b8adc in TabStrip::OnMouseDragged(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\
tabs\tab_strip.cc:3683:3
   #14 0x7febda736d6 in views::View::ProcessMouseDragged(class ui::MouseEvent *) C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:2998:
```

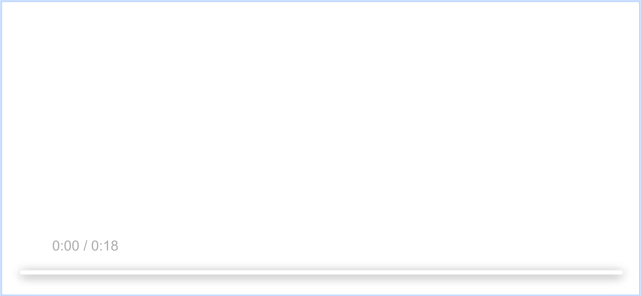
```
9
    #15 0x7febe907f74 in ui::EventHandler::OnEvent(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37:5
    #16 0x7febe906979 in ui::EventDispatcher::DispatchEvent(class ui::EventHandler *, class ui::Event *) C:\b\s\w\ir\cache\builder\src
\ui\events\event_dispatcher.cc:191:12
    #17 0x7febe905de8 in ui::EventDispatcher::ProcessEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\builder\src\u
i\events\event_dispatcher.cc:140:5
    #18 0x7febe9057d4 in ui::EventDispatcherDelegate::DispatchEventToTarget(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\ca
che\builder\src\ui\events\event_dispatcher.cc:84:14
    #19 0x7febe905418 in ui::EventDispatcherDelegate::DispatchEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\buil
der\src\ui\events\event_dispatcher.cc:56:15
    #20 0x7fec02a15cf in views::internal::RootView::OnMouseDragged(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\ui\view
s\widget\root_view.cc:457:9
    #21 0x7febda9b0bd in views::Widget::OnMouseEvent(class ui::MouseEvent *) C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1
335:22
    #22 0x7febe907f74 in ui::EventHandler::OnEvent(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37:5
    #23 0x7febe906979 in ui::EventDispatcher::DispatchEvent(class ui::EventHandler *, class ui::Event *) C:\b\s\w\ir\cache\builder\src
\ui\events\event_dispatcher.cc:191:12
    #24 0x7febe905de8 in ui::EventDispatcher::ProcessEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\builder\src\u
i\events\event_dispatcher.cc:140:5
    #25 0x7febe9057d4 in ui::EventDispatcherDelegate::DispatchEventToTarget(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\ca
che\builder\src\ui\events\event_dispatcher.cc:84:14
    #26 0x7febe905418 in ui::EventDispatcherDelegate::DispatchEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\buil
der\src\ui\events\event_dispatcher.cc:56:15
    #27 0x7fec31feea0 in ui::EventProcessor::OnEventFromSource(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_proces
sor.cc:49:17
    #28 0x7fec0290f03 in ui::EventSource::DeliverEventToSink(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_source.c
c:113:16
    #29 0x7fec0290b5d in ui::EventSource::SendEventToSinkFromRewriter(class ui::Event const *, class ui::EventRewriter const *) C:\b\s
\w\ir\cache\builder\src\ui\events\event_source.cc:138:12
    #30 0x7fec029065b in ui::EventSource::SendEventToSink(class ui::Event const *) C:\b\s\w\ir\cache\builder\src\ui\events\event_sourc
e.cc:107:10
    #31 0x7fec31fbd01 in views::DesktopWindowTreeHostWin::HandleMouseEvent(class ui::MouseEvent *) C:\b\s\w\ir\cache\builder\src\ui\vi
ews\widget\desktop_aura\desktop_window_tree_host_win.cc:958:3
    #32 0x7fec70737c9 in views::HWNDMessageHandler::HandleMouseEventInternal(unsigned int, unsigned __int64, __int64, bool) C:\b\s\w\i
r\cache\builder\src\ui\views\win\hwnd_message_handler.cc:3130:26
    #33 0x7fec706cc0b in views::HWNDMessageHandler::OnMouseRange C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:19
56
    #34 0x7fec706cc0b in views::HWNDMessageHandler::_ProcessWindowMessage(struct HWND__*, unsigned int, unsigned __int64, __int64, __i
nt64 &, unsigned long) C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.h:356:5
    #35 0x7fec706c325 in views::HWNDMessageHandler::OnWndProc(unsigned int, unsigned __int64, __int64) C:\b\s\w\ir\cache\builder\src\u
i\views\win\hwnd_message_handler.cc:1009:7
    #36 0x7fec0a296dc in gfx::WindowImpl::WndProc(struct HWND__*, unsigned int, unsigned __int64, __int64) C:\b\s\w\ir\cache\builder\s
rc\ui\gfx\win\window_impl.cc:305:18
    #37 0x7fec0a28083 in base::win::WrappedWindowProc<&gfx::WindowImpl::WndProc(struct HWND__*, unsigned int, unsigned __int64, __int6
4)>(struct HWND__*, unsigned int, unsigned __int64, __int64) C:\b\s\w\ir\cache\builder\src\base\win\wrapped_window_proc.h:74:10
    #38 0x4539bd0  (C:\Windows\system32\USER32.dll+0x78c39bd0)
    #39 0x45398d9  (C:\Windows\system32\USER32.dll+0x78c398d9)
    #40 0x7febdca7fb3 in base::MessagePumpForUI::ProcessMessageHelper(struct tagMSG const &) C:\b\s\w\ir\cache\builder\src\base\messag
e_loop\message_pump_win.cc:537:3
    #41 0x7febdca5eba in base::MessagePumpForUI::ProcessNextWindowsMessage(void) C:\b\s\w\ir\cache\builder\src\base\message_loop\messa
ge_pump_win.cc:504:31
    #42 0x7febdca57ac in base::MessagePumpForUI::DoRunLoop(void) C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:2
19:35
    #43 0x7febdca332a in base::MessagePumpWin::Run(class base::MessagePump::Delegate *) C:\b\s\w\ir\cache\builder\src\base\message_loo
p\message_pump_win.cc:80:3
    #44 0x7fec03af7cf in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, class base::TimeDelta) C:\b\
s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460:12
    #45 0x7febdba8303 in base::RunLoop::Run(class base::Location const &) C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:133:14
    #46 0x7fec04ea238 in ChromeBrowserMainParts::MainMessageLoopRun(int *) C:\b\s\w\ir\cache\builder\src\chrome\browser\chrome_browser
_main.cc:1740:15
    #47 0x7feb77dfd01 in content::BrowserMainLoop::RunMainMessageLoopParts(void) C:\b\s\w\ir\cache\builder\src\content\browser\browser
_main_loop.cc:970:29
    #48 0x7feb77e5a8f in content::BrowserMainRunnerImpl::Run(void) C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_i
mpl.cc:150:15
    #49 0x7feb77d8512 in content::BrowserMain(struct content::MainFunctionParams const &) C:\b\s\w\ir\cache\builder\src\content\browse
r\browser_main.cc:47:28
    #50 0x7febd963353 in content::RunBrowserProcessMain(struct content::MainFunctionParams const &, class content::ContentMainDelegate
 *) C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:516:10
    #51 0x7febd965cab in content::ContentMainRunnerImpl::RunBrowser(struct content::MainFunctionParams &, bool) C:\b\s\w\ir\cache\buil
der\src\content\app\content_main_runner_impl.cc:997:10
    #52 0x7febd965027 in content::ContentMainRunnerImpl::Run(bool) C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.
cc:875:12
    #53 0x7febd96220e in content::RunContentProcess(struct content::ContentMainParams const &, class content::ContentMainRunner *) C:\
b\s\w\ir\cache\builder\src\content\app\content_main.cc:372:36
    #54 0x7febd9627f8 in content::ContentMain(struct content::ContentMainParams const &) C:\b\s\w\ir\cache\builder\src\content\app\con
tent_main.cc:398:10
    #55 0x7feb3b8145a in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:141:12
    #56 0x13ffb5ac1 in MainDllLoader::Launch(struct HINSTANCE__*, class base::TimeTicks) C:\b\s\w\ir\cache\builder\src\chrome\app\main
_dll_loader_win.cc:169:12
    #57 0x13ffb29b7 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:351:20
    #58 0x140390dbf in invoke_main d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:78
    #59 0x140390dbf in __scrt_common_main_seh d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #60 0x776c652c  (C:\Windows\system32\kernel32.dll+0x78d3652c)
    #61 0x778fc520  (C:\Windows\SYSTEM32\ntdll.dll+0x78e7c520)

0x010741df3fe0 is located 16 bytes inside of 32-byte region [0x010741df3fd0,0x010741df3ff0)
allocated by thread T0 here:
    #0 0x1400542ab in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7fecfffacaa in operator new(unsigned __int64) d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7fec22f6a1f in std::__1::__libcpp_allocate C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\new:253
    #3 0x7fec22f6a1f in std::__1::allocator<std::unique_ptr<TabStripModel::WebContentsData,std::default_delete<TabStripModel::WebConte
ntsData> > >::allocate C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory:1853
    #4 0x7fec22f6a1f in std::__1::allocator_traits<std::allocator<std::unique_ptr<TabStripModel::WebContentsData,std::default_delete<T
abStripModel::WebContentsData> > > >::allocate C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory:1570
    #5 0x7fec22f6a1f in std::__1::__split_buffer<std::unique_ptr<TabStripModel::WebContentsData,std::default_delete<TabStripModel::Web
ContentsData> >,std::allocator<std::unique_ptr<TabStripModel::WebContentsData,std::default_delete<TabStripModel::WebContentsData> > >
&>::__split_buffer C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\__split_buffer:318
    #6 0x7fec22f6a1f in std::__1::vector<class std::__1::unique_ptr<class TabStripModel::WebContentsData, struct std::__1::default_del
ete<class TabStripModel::WebContentsData>>, class std::__1::allocator<class std::__1::unique_ptr<class TabStripModel::WebContentsData,
 struct std::__1::default_delete<class TabStripModel::WebContentsData>>>>::insert(class std::__1::__wrap_iter<class std::__1::unique_p
tr<class TabStripModel::WebContentsData, struct std::__1::default_delete<class TabStripModel::WebContentsData>> const *>, class std::_
_1::unique_ptr<class TabStripModel::WebContentsData, struct std::__1::default_delete<class TabStripModel::WebContentsData>> &&) C:\b\s
\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\vector:1825:53
```

```
    #7 0x7fec22de5c1 in TabStripModel::InsertWebContentsAtImpl(int, class std::__1::unique_ptr<class content::WebContents, struct std:
:__1::default_delete<class content::WebContents>>, int, class base::Optional<class tab_groups::TabGroupId>) C:\b\s\w\ir\cache\builder\
src\chrome\browser\ui\tabs\tab_strip_model.cc:1715:18
    #8 0x7fec22eaed2 in TabStripModel::AddWebContents(class std::__1::unique_ptr<class content::WebContents, struct std::__1::default_
delete<class content::WebContents>>, int, enum ui::PageTransition, int, class base::Optional<class tab_groups::TabGroupId>) C:\b\s\w\i
r\cache\builder\src\chrome\browser\ui\tabs\tab_strip_model.cc:982:3
    #9 0x7febfeee07e in Navigate(struct NavigateParams *) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_navigator.cc:702:41
    #10 0x7fec38a675d in chrome::AddTabAt(class Browser *, class GURL const &, int, bool, class base::Optional<class tab_groups::TabGr
oupId>) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_tabstrip.cc:40:3
    #11 0x7fec3f41e2d in chrome::BrowserTabStripModelDelegate::AddTabAt(class GURL const &, int, bool, class base::Optional<class tab_
groups::TabGroupId>) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_tab_strip_model_delegate.cc:53:3
    #12 0x7fec7999411 in BrowserTabStripController::CreateNewTab(void) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs\brow
ser_tab_strip_controller.cc:464:23
    #13 0x7fec79b50ce in TabStrip::NewTabButtonPressed(class ui::Event const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\
tabs\tab_strip.cc:2613:16
    #14 0x7fecaa236ec in NewTabButton::NotifyClick(class ui::Event const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\tabs
\new_tab_button.cc:140:16
    #15 0x7fec025549a in views::ButtonController::OnMouseReleased(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\ui\views
\controls\button\button_controller.cc:58:34
    #16 0x7fecaa234c2 in NewTabButton::OnMouseReleased(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\v
iews\tabs\new_tab_button.cc:115:25
    #17 0x7febda73b0c in views::View::ProcessMouseReleased(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\ui\views\view.c
c:3021:5
    #18 0x7febe907f74 in ui::EventHandler::OnEvent(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37:5
    #19 0x7fec7015846 in ui::ScopedTargetHandler::OnEvent(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\scoped_target_han
dler.cc:28:24
    #20 0x7febe906979 in ui::EventDispatcher::DispatchEvent(class ui::EventHandler *, class ui::Event *) C:\b\s\w\ir\cache\builder\src
\ui\events\event_dispatcher.cc:191:12
    #21 0x7febe905de8 in ui::EventDispatcher::ProcessEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\builder\src\u
i\events\event_dispatcher.cc:140:5
    #22 0x7febe9057d4 in ui::EventDispatcherDelegate::DispatchEventToTarget(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\ca
che\builder\src\ui\events\event_dispatcher.cc:84:14
    #23 0x7febe905418 in ui::EventDispatcherDelegate::DispatchEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\buil
der\src\ui\events\event_dispatcher.cc:56:15
    #24 0x7fec02a18f2 in views::internal::RootView::OnMouseReleased(class ui::MouseEvent const &) C:\b\s\w\ir\cache\builder\src\ui\vie
ws\widget\root_view.cc:475:9
    #25 0x7febda9b6ba in views::Widget::OnMouseEvent(class ui::MouseEvent *) C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1
318:20
    #26 0x7febe907f74 in ui::EventHandler::OnEvent(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37:5
    #27 0x7febe906979 in ui::EventDispatcher::DispatchEvent(class ui::EventHandler *, class ui::Event *) C:\b\s\w\ir\cache\builder\src
\ui\events\event_dispatcher.cc:191:12
    #28 0x7febe905de8 in ui::EventDispatcher::ProcessEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\builder\src\u
i\events\event_dispatcher.cc:140:5
    #29 0x7febe9057d4 in ui::EventDispatcherDelegate::DispatchEventToTarget(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\ca
che\builder\src\ui\events\event_dispatcher.cc:84:14
    #30 0x7febe905418 in ui::EventDispatcherDelegate::DispatchEvent(class ui::EventTarget *, class ui::Event *) C:\b\s\w\ir\cache\buil
der\src\ui\events\event_dispatcher.cc:56:15
    #31 0x7fec31feea0 in ui::EventProcessor::OnEventFromSource(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_proces
sor.cc:49:17
    #32 0x7fec0290f03 in ui::EventSource::DeliverEventToSink(class ui::Event *) C:\b\s\w\ir\cache\builder\src\ui\events\event_source.c
c:113:16

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 C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory:2602 in
 std::__1::unique_ptr<TabStripModel::WebContentsData,std::default_delete<TabStripModel::WebContentsData> >::operator->
Shadow bytes around the buggy address:
  0x002229ebe7a0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fa
  0x002229ebe7b0: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x002229ebe7c0: fd fd fa fa fd fd fd fa fa fa fd fd fd fa fa fa
  0x002229ebe7d0: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fd
  0x002229ebe7e0: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
=>0x002229ebe7f0: fd fd fa fa fd fd fd fd fa fa 00 00[fc]fc fa fa
  0x002229ebe800: fd fd fd fd fa fa fd fd fd fa fa fd fd fd fd
  0x002229ebe810: fa fa fd fd fd fd fa fa fd fd fd fa fa fa fd fd
  0x002229ebe820: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x002229ebe830: fd fd fd fa fa fa fd fd fd fd fa fa fd fd fd fd
  0x002229ebe840: fa fa fd fd fd fa fa fa fd fd fd fa fa fa fd fd
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
==5516==ABORTING
```

screen.mov
6.1 MB View Download



poc.html
176 bytes View Download

Comment 1 by sheriffbot on Sat, Feb 6, 2021, 7:28 PM EST Project Member

Labels: external_security_report

Comment 2 by tsepez@chromium.org on Mon, Feb 8, 2021, 12:59 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: tbergquist@google.com
Labels: Security_Severity-High Security_Impact-Stable OS-Windows Pri-1
Components: UI>Browser>TabStrip

Related to 1173269 ?

Comment 3 by tbergquist@google.com on Mon, Feb 8, 2021, 1:36 PM EST Project Member

Owner: tbergquist@chromium.org

Comment 4 by tbergquist@chromium.org on Mon, Feb 8, 2021, 1:48 PM EST Project Member

Status: Started (was: Assigned)

Yes it is related! Looks like reverts with a group involved are making it past the crash in 1173269 only to founder for the same basic reason shortly thereafter.

I'll post a candidate fix shortly.

Comment 5 by tbergquist@chromium.org on Mon, Feb 8, 2021, 1:59 PM EST Project Member

Cc: connily@chromium.org

CL posted! CCing Connie who's going to help test it (I can't repro this category of issues on my mac)

Comment 6 by bugdroid on Mon, Feb 8, 2021, 4:02 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4630d6f564bf86f0225383f9a4914c55fc8da55f

commit 4630d6f564bf86f0225383f9a4914c55fc8da55f
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Mon Feb 08 21:01:41 2021

Fix RevertDragAt losing track of tabs in some cases.

~~Bug: 1175500~~
Change-Id: I9addf8bd76c38d647a8009cd6805be9af48ba1b9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2682744
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Cr-Commit-Position: refs/heads/master@{#851880}

[modify] https://crrev.com/4630d6f564bf86f0225383f9a4914c55fc8da55f/chrome/browser/ui/views/tabs/tab_drag_controller.cc

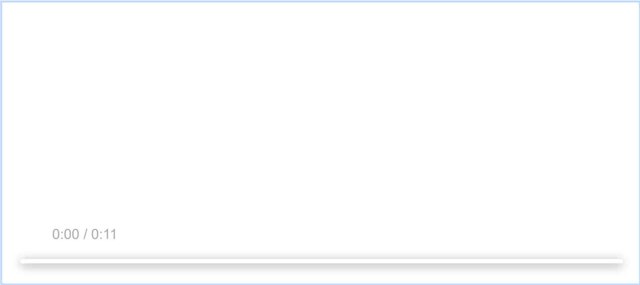
Comment 7 by tbergquist@chromium.org on Mon, Feb 8, 2021, 4:12 PM EST Project Member

Status: Fixed (was: Started)

Comment 8 by chrom...@gmail.com on Mon, Feb 8, 2021, 6:25 PM EST

Verified on Chromium 90.0.4413.0 revision#851887. Nice work!

fixed.mov
2.4 MB View Download



Comment 9 by sheriffbot on Tue, Feb 9, 2021, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 10 by sheriffbot on Tue, Feb 9, 2021, 12:48 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 11 by sheriffbot on Tue, Feb 9, 2021, 1:57 PM EST Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 12 by sheriffbot on Tue, Feb 9, 2021, 2:18 PM EST Project Member
Labels: Merge-Request-89 Merge-Request-88

Requesting merge to stable M88 because latest trunk commit (851880) appears to be after stable branch point (827102).

Requesting merge to beta M89 because latest trunk commit (851880) appears to be after beta branch point (843830).

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

Comment 13 by pbommana@google.com on Tue, Feb 9, 2021, 3:25 PM EST Project Member
Cc: adetaylor@chromium.org pbomm...@chromium.org

+adetaylor(Security TPM) for merge decision.

Comment 14 by sheriffbot on Tue, Feb 9, 2021, 4:07 PM EST Project Member
Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.
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 15 by adetaylor@chromium.org on Tue, Feb 9, 2021, 4:35 PM EST Project Member
Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389.

Comment 16 by tbergquist@chromium.org on Tue, Feb 9, 2021, 6:08 PM EST Project Member

Hi @adetaylor, this bugfix depends on another one: https://bugs.chromium.org/p/chromium/issues/detail?id=1173269
I can't merge this one without merging that one as well.

Comment 17 by bugdroid on Wed, Feb 10, 2021, 2:27 AM 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/+/e6698f21a5ff109c619c5e9839af2b9e8d5aa2e8

commit e6698f21a5ff109c619c5e9839af2b9e8d5aa2e8
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Wed Feb 10 07:27:00 2021

Fix RevertDragAt losing track of tabs in some cases.

(cherry picked from commit c0b715ae52a2966f2baf49483b613a6c3c164246)

~~Bug: 1175500~~
Change-Id: I9addf8bd76c38d647a8009cd6805be9af48ba1b9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2682744
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#851880}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2686099
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@{#882}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/e6698f21a5ff109c619c5e9839af2b9e8d5aa2e8/chrome/browser/ui/views/tabs/tab_drag_controller.cc

Comment 18 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:23 PM EST Project Member
Labels: -Merge-Request-88 Merge-Approved-88

Approving merge to M88, branch 4324. Please merge by the end of Thursday PST to get into next Tuesday's release.

Comment 19 by bugdroid on Wed, Feb 10, 2021, 6:36 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/+/c711d711fa06c7658f0d9d3835ab029a3b9ffdba

commit c711d711fa06c7658f0d9d3835ab029a3b9ffdba
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Wed Feb 10 23:36:16 2021

Fix RevertDragAt losing track of tabs in some cases.

(cherry picked from commit 4630d6f564bf86f0225383f9a4914c55fc8da55f)

~~Bug: 1175500~~
Change-Id: I9addf8bd76c38d647a8009cd6805be9af48ba1b9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2682744
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#851880}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2688380
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/4324@{#2165}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/c711d711fa06c7658f0d9d3835ab029a3b9ffdba/chrome/browser/ui/views/tabs/tab_drag_controller.cc

Comment 20 by adetaylor@google.com on Fri, Feb 12, 2021, 7:35 PM EST Project Member

Labels: Release-3-M88

Comment 21 by amyressler@google.com on Wed, Feb 17, 2021, 7:12 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 22 by amyressler@google.com on Wed, Feb 17, 2021, 7:27 PM EST Project Member

Hello, Khalil! The VRP Panel has decided to award you $7,500 for this report. Nice work!

Comment 23 by achuith@chromium.org on Thu, Feb 18, 2021, 8:14 PM EST Project Member

Labels: LTS-Security-86 Merge-Request-86-LTS

Comment 24 by awhalley@google.com on Fri, Feb 19, 2021, 5:34 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@google.com on Mon, Feb 22, 2021, 4:31 PM EST Project Member

Labels: CVE-2021-21155 CVE_description-missing

Comment 26 by amyressler@google.com on Mon, Feb 22, 2021, 4:33 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 27 by gianluca@google.com on Tue, Feb 23, 2021, 4:27 PM EST Project Member

Labels: -Merge-Request-86-LTS LTS-Merge-Request-86

Comment 28 by gianluca@google.com on Tue, Feb 23, 2021, 5:15 PM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 29 by achuith@chromium.org on Tue, Feb 23, 2021, 5:33 PM EST Project Member

Labels: -LTS-Merge-Request-86

Comment 30 by bugdroid on Tue, Feb 23, 2021, 6:59 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ab921a71a7180f490bb1ef600b4e124fbc6ef020

commit ab921a71a7180f490bb1ef600b4e124fbc6ef020
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Tue Feb 23 23:58:03 2021

Fix RevertDragAt losing track of tabs in some cases.

(cherry picked from commit 4630d6f564bf86f0225383f9a4914c55fc8da55f)

~~Bug: 1175500~~
Change-Id: I9addf8bd76c38d647a8009cd6805be9af48ba1b9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2682744
Reviewed-by: Connie Wan <connily@chromium.org>
Commit-Queue: Taylor Bergquist <tbergquist@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#851880}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2705982
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1549}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/ab921a71a7180f490bb1ef600b4e124fbc6ef020/chrome/browser/ui/views/tabs/tab_drag_controller.cc

Comment 31 by asumaneev@google.com on Tue, Mar 2, 2021, 10:41 AM EST Project Member

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

Comment 32 by sheriffbot on Tue, May 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