☆ Starred by 2 users

| | |
|---|---|
| **Owner:** | tbergquist@chromium.org |
| **CC:** | solomonkinard@chromium.org<br>pbos@chromium.org<br>tbergquist@chromium.org<br>cyan@chromium.org<br>kylixrd@chromium.org<br>connily@chromium.org<br>pkasting@chromium.org<br>sky@chromium.org |
| **Status:** | Verified *(Closed)* |
| **Components:** | ---- |
| **Modified:** | Aug 28, 2021 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Windows, Mac |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
Merge-na
Security_Impact-Stable
Security_Severity-Medium
Hotlist-Merge-Approved
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
M-91
LTS-Security-86
LTS-Security-NotApplicable-86
Target-91
external_security_report
LTS-Merged-90
LTS-Security-90
Release-0-M91
CVE-2021-30543

### Issue 1203607: Security: Heap-use-after-free in TabStripLayoutHelper::CalculateMinimumWidth

Reported by chrom...@gmail.com on Wed, Apr 28, 2021, 4:27 AM EDT

Code

Chrome Version: 92.0.4490.0 (Official Build) canary (x86_64) and stable
Operating System: MacOS

**REPRODUCTION CASE**

1. Install the extension.
2. Click on the first color indicator icon and drag the tab out of the tab strip.
3. Then drag it back to the tab strip.

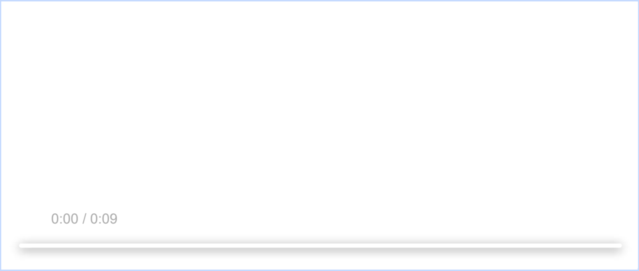
```
==1071==ERROR: AddressSanitizer: heap-use-after-free on address 0x61800020bf30 at pc 0x00012d24ed7d bp 0x7fff55a85190 sp 0x7fff55a85188
READ of size 1 at 0x61800020bf30 thread T0
    #0 0x12d24ed7c in TabStripLayoutHelper::CalculateIdealBounds(base::Optional<int>) optional.h:165
    #1 0x12d250e2a in TabStripLayoutHelper::CalculateMinimumWidth() tab_strip_layout_helper.cc:229
    #2 0x12d22c136 in TabStrip::GetMinimumSize() const tab_strip.cc:2474
    #3 0x12bc8dd34 in views::(anonymous namespace)::GetPreferredSize(views::MinimumFlexSizeRule, views::MaximumFlexSizeRule, views::MinimumFlexSizeRule,
views::MaximumFlexSizeRule, bool, views::View const*, views::SizeBounds const&) flex_layout_types.cc:85
    #4 0x12bc8f240 in base::internal::Invoker<base::internal::BindState<gfx::Size (*)(views::MinimumFlexSizeRule, views::MaximumFlexSizeRule,
views::MinimumFlexSizeRule, views::MaximumFlexSizeRule, bool, views::View const*, views::SizeBounds const&), views::MinimumFlexSizeRule,
views::MaximumFlexSizeRule, views::MinimumFlexSizeRule, views::MaximumFlexSizeRule, bool>, gfx::Size (views::View const*, views::SizeBounds
const&)>::Run(base::internal::BindStateBase*, views::View const*, views::SizeBounds const&) bind_internal.h:404
    #5 0x12bc84780 in views::FlexLayout::GetPreferredSizeForRule(base::RepeatingCallback<gfx::Size (views::View const*, views::SizeBounds const&)> const&, views::View
const*, views::SizeBound const&) const callback.h:169
    #6 0x12bc7eb6e in views::FlexLayout::InitializeChildData(views::NormalizedSizeBounds const&, views::FlexLayout::FlexLayoutData&, std::__1::map<int,
std::__1::list<unsigned long, std::__1::allocator<unsigned long> >, std::__1::less<int>, std::__1::allocator<std::__1::pair<int const, std::__1::list<unsigned long,
std::__1::allocator<unsigned long> > > > >&) const flex_layout.cc:545
    #7 0x12bc7d0ef in views::FlexLayout::CalculateProposedLayout(views::SizeBounds const&) const flex_layout.cc:418
    #8 0x12bcb2d42 in views::LayoutManagerBase::GetAvailableSize(views::View const*, views::View const*) const layout_manager_base.cc:103
    #9 0x12bd15456 in views::View::GetAvailableSize(views::View const*) const view.cc:536
    #10 0x12cdb0315 in TabStripRegionView::GetTabStripAvailableWidth() const tab_strip_region_view.cc:381
    #11 0x12d21c8dc in TabStrip::OnGroupVisualsChanged(tab_groups::TabGroupId const&, tab_groups::TabGroupVisualData const*, tab_groups::TabGroupVisualData
const*) callback.h:169
    #12 0x12d1809b9 in BrowserTabStripController::OnTabGroupChanged(TabGroupChange const&) browser_tab_strip_controller.cc:730
    #13 0x12c67c40f in TabStripModel::ChangeTabGroupVisuals(tab_groups::TabGroupId const&, TabGroupChange::VisualsChange const&) tab_strip_model.cc:1219
    #14 0x12c6566d3 in TabGroup::AddTab() tab_group.cc:68
    #15 0x12c679299 in TabStripModel::GroupTab(int, tab_groups::TabGroupId const&) tab_strip_model.cc:2257
    #16 0x12c663f2c 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:1782
    #17 0x12c66312e in TabStripModel::InsertWebContentsAt(int, std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, int,
base::Optional<tab_groups::TabGroupId>) tab_strip_model.cc:388
    #18 0x12d1c2603 in TabDragController::Attach(TabDragContext*, gfx::Point const&, bool) tab_drag_controller.cc:1222
    #19 0x12d1c77e2 in TabDragController::RunMoveLoop(gfx::Vector2d const&) tab_drag_controller.cc:1447
    #20 0x12d1cc239 in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) tab_drag_controller.cc:1390
    #21 0x12d1c9e5f in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) tab_drag_controller.cc:865
    #22 0x12d1c7eeb in TabDragController::ContinueDragging(gfx::Point const&) tab_drag_controller.cc:831
    #23 0x12d1c0cc3 in TabDragController::Drag(gfx::Point const&) tab_drag_controller.cc:604
    #24 0x12d226117 in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) tab_strip.cc:456
    #25 0x12d2336cb in TabStrip::OnMouseDragged(ui::MouseEvent const&) tab_strip.cc:3745
    #26 0x12bd2485d in views::View::ProcessMouseDragged(ui::MouseEvent*) view.cc:2996
    #27 0x123bb083f in ui::EventHandler::OnEvent(ui::Event*) event_handler.cc
    #28 0x123baeca2 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
    #29 0x123bae550 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
    #30 0x12bd5eeda in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) root_view.cc:457
    #31 0x12bd7a5d7 in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1347
    #32 0x12bdb705c in non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event> >)
native_widget_mac_ns_window_host.mm:809
    #33 0x127f9cebb in -[BridgedContentView mouseEvent:] bridged_content_view.mm:595
    #34 0x127f9a36d in -[BridgedContentView processCapturedMouseEvent:] bridged_content_view.mm:308
    #35 0x127fa823b in ___ZN12remote_cocoa17CocoaMouseCapture14ActiveEventTap4InitEv_block_invoke mouse_capture.mm:91
    #36 0x7fff958d87f9 in _NSSendEventToObservers+0x173 (AppKit:x86_64+0x1c77f9)
    #37 0x7fff95ed123e in -[NSApplication(NSEvent) sendEvent:]+0x36 (AppKit:x86_64+0x7c023e)
    #38 0x1217a9104 in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:335
    #39 0x120597569 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xbdd9569)
    #40 0x1217a847e in -[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:319
    #41 0x7fff9574c3d6 in -[NSApplication run]+0x3e9 (AppKit:x86_64+0x3b3d6)
    #42 0x1205abd4a in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*) message_pump_mac.mm:717
    #43 0x1205a7938 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*) message_pump_mac.mm:157
    #44 0x1204ba40b in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
thread_controller_with_message_pump_impl.cc:460
    #45 0x1203f627e in base::RunLoop::Run(base::Location const&) run_loop.cc:133
    #46 0x118ef8a08 in content::BrowserMainLoop::RunMainMessageLoop() browser_main_loop.cc:990
    #47 0x118efd231 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:150
    #48 0x118ef166c in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:47
    #49 0x1201c90f6 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content_main_runner_impl.cc:598
    #50 0x1201c8394 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:956
    #51 0x1201c5526 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content_main.cc:372
    #52 0x1201c5b3c in content::ContentMain(content::ContentMainParams const&) content_main.cc:398
    #53 0x1147c5005 in ChromeMain chrome_main.cc:141
    #54 0x10a1771ef in main chrome_exe_main_mac.cc:114
    #55 0x7fffad8ac234 in start+0x0 (libdyld.dylib:x86_64+0x5234)

0x61800020bf30 is located 688 bytes inside of 840-byte region [0x61800020bc80,0x61800020bfc8)
freed by thread T0 here:
    #0 0x10a373ff9  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x44ff9)
    #1 0x12d1f1dbb in TabGroupViews::~TabGroupViews() memory:1335
    #2 0x12d21bb64 in TabStrip::OnGroupCreated(tab_groups::TabGroupId const&) memory:1596
    #3 0x12d180508 in BrowserTabStripController::OnTabGroupChanged(TabGroupChange const&) browser_tab_strip_controller.cc:689
    #4 0x12c67ac6c in TabStripModel::CreateTabGroup(tab_groups::TabGroupId const&) tab_strip_model.cc:1198
    #5 0x12c65664a in TabGroup::AddTab() tab_group.cc:65
    #6 0x12c679299 in TabStripModel::GroupTab(int, tab_groups::TabGroupId const&) tab_strip_model.cc:2257
    #7 0x12c663f2c 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:1782
    #8 0x12c66312e in TabStripModel::InsertWebContentsAt(int, std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, int,
base::Optional<tab_groups::TabGroupId>) tab_strip_model.cc:388
    #9 0x12d1c2603 in TabDragController::Attach(TabDragContext*, gfx::Point const&, bool) tab_drag_controller.cc:1222
    #10 0x12d1c77e2 in TabDragController::RunMoveLoop(gfx::Vector2d const&) tab_drag_controller.cc:1447
    #11 0x12d1cc239 in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) tab_drag_controller.cc:1390
    #12 0x12d1c9e5f in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) tab_drag_controller.cc:865
    #13 0x12d1c7eeb in TabDragController::ContinueDragging(gfx::Point const&) tab_drag_controller.cc:831
    #14 0x12d1c0cc3 in TabDragController::Drag(gfx::Point const&) tab_drag_controller.cc:604
    #15 0x12d226117 in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) tab_strip.cc:456
    #16 0x12d2336cb in TabStrip::OnMouseDragged(ui::MouseEvent const&) tab_strip.cc:3745
    #17 0x12bd2485d in views::View::ProcessMouseDragged(ui::MouseEvent*) view.cc:2996
    #18 0x123bb083f in ui::EventHandler::OnEvent(ui::Event*) event_handler.cc
    #19 0x123baeca2 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
    #20 0x123bae550 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
    #21 0x12bd5eeda in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) root_view.cc:457
    #22 0x12bd7a5d7 in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1347
    #23 0x12bdb705c in non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event> >)
native_widget_mac_ns_window_host.mm:809
    #24 0x127f9cebb in -[BridgedContentView mouseEvent:] bridged_content_view.mm:595
    #25 0x127f9a36d in -[BridgedContentView processCapturedMouseEvent:] bridged_content_view.mm:308
    #26 0x127fa823b in ___ZN12remote_cocoa17CocoaMouseCapture14ActiveEventTap4InitEv_block_invoke mouse_capture.mm:91
    #27 0x7fff958d87f9 in _NSSendEventToObservers+0x173 (AppKit:x86_64+0x1c77f9)
    #28 0x7fff95ed123e in -[NSApplication(NSEvent) sendEvent:]+0x36 (AppKit:x86_64+0x7c023e)
    #29 0x1217a9104 in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:335

previously allocated by thread T0 here:
    #0 0x10a373eb0  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x44eb0)
    #1 0x1202eff97 in operator new(unsigned long) new.cpp:67
    #2 0x12d1f1aac in TabGroupViews::TabGroupViews(TabStrip*, tab_groups::TabGroupId const&) memory:2006
    #3 0x12d21ba52 in TabStrip::OnGroupCreated(tab_groups::TabGroupId const&) tab_strip.cc:1487
    #4 0x12d180508 in BrowserTabStripController::OnTabGroupChanged(TabGroupChange const&) browser_tab_strip_controller.cc:689
    #5 0x12c67ac6c in TabStripModel::CreateTabGroup(tab_groups::TabGroupId const&) tab_strip_model.cc:1198
    #6 0x12c65664a in TabGroup::AddTab() tab_group.cc:65
    #7 0x12c679299 in TabStripModel::GroupTab(int, tab_groups::TabGroupId const&) tab_strip_model.cc:2257
    #8 0x12c686b96 in TabStripModel::MoveAndSetGroup(int, int, base::Optional<tab_groups::TabGroupId>) tab_strip_model.cc:2198
    #9 0x12c676b2c in TabStripModel::MoveTabsAndSetGroupImpl(std::__1::vector<int, std::__1::allocator<int> > const&, int, base::Optional<tab_groups::TabGroupId>)
tab_strip_model.cc:2167
    #10 0x12c675b69 in TabStripModel::AddToNewGroupImpl(std::__1::vector<int, std::__1::allocator<int> > const&, tab_groups::TabGroupId const&) tab_strip_model.cc:2114
    #11 0x12c675595 in TabStripModel::AddToNewGroup(std::__1::vector<int, std::__1::allocator<int> > const&) tab_strip_model.cc:1085
    #12 0x12b05a4eb in extensions::TabsGroupFunction::Run() tabs_api.cc:1844
    #13 0x11b28d4d7 in ExtensionFunction::RunWithValidation() extension_function.cc:471
    #14 0x11b2964f5 in extensions::ExtensionFunctionDispatcher::DispatchWithCallbackInternal(extensions::mojom::RequestParams const&, content::RenderFrameHost*, int,
base::OnceCallback<void (ExtensionFunction::ResponseType, base::ListValue const&, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >
const&)>) extension_function_dispatcher.cc:384
    #15 0x11b29551c in extensions::ExtensionFunctionDispatcher::Dispatch(extensions::mojom::RequestParams const&, content::RenderFrameHost*, int)
extension_function_dispatcher.cc:254
    #16 0x11b30e406 in extensions::ExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
extension_web_contents_observer.cc:346
    #17 0x12b0e0db3 in extensions::ChromeExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
chrome_extension_web_contents_observer.cc:101
    #18 0x11a0404a7 in content::WebContentsImpl::OnMessageReceived(content::RenderFrameHostImpl*, IPC::Message const&) web_contents_impl.cc:1120
    #19 0x119b27946 in content::RenderFrameHostImpl::OnMessageReceived(IPC::Message const&) render_frame_host_impl.cc:1986
    #20 0x123aa542d in IPC::ChannelProxy::Context::OnDispatchMessage(IPC::Message const&) ipc_channel_proxy.cc:325
    #21 0x1204799e3 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) callback.h:101
    #22 0x1204b91da in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:351
    #23 0x1204b89f7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:264
    #24 0x1205aa368 in ___ZN4base24MessagePumpCFRunLoopBase13RunWorkSourceEPv_block_invoke message_pump_mac.mm:384
    #25 0x120597569 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xbdd9569)
    #26 0x1205a8b15 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:360
    #27 0x7fff97c83e50 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64+0xa4e50)
    #28 0x7fff97c650cb in __CFRunLoopDoSources0+0x22b (CoreFoundation:x86_64+0x860cb)
    #29 0x7fff97c645b5 in __CFRunLoopRun+0x3a5 (CoreFoundation:x86_64+0x855b5)

SUMMARY: AddressSanitizer: heap-use-after-free optional.h:165 in TabStripLayoutHelper::CalculateIdealBounds(base::Optional<int>)
Shadow bytes around the buggy address:
  0x1c3000041790: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c30000417a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c30000417b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c30000417c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c30000417d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x1c30000417e0: fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd
  0x1c30000417f0: fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa
  0x1c3000041800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c3000041810: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3000041820: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3000041830: fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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
```

**screen .mov**
6.4 MB View Download



**poc.zip**
6.6 KB Download

Comment 1 by sheriffbot on Wed, Apr 28, 2021, 4:29 AM EDT Project Member

**Labels:** external_security_report

Comment 2 by ajgo@google.com on Wed, Apr 28, 2021, 12:57 PM EDT Project Member

**Status:** Untriaged (was: Unconfirmed)
**Cc:** connily@chromium.org cyan@chromium.org kylixrd@chromium.org pkasting@chromium.org sky@chromium.org tbergquist@chromium.org
**Labels:** Security_Severity-Medium Security_Impact-Stable OS-Mac Pri-2
**Components:** UI>Browser>TabStrip

Hi tab strip people - could you suggest someone to take a look at this use-after-free.

Setting severity=medium as significant user interaction is required.

**background.js**
42 bytes View Download

**manifest.json**
194 bytes View Download

**poc.html**
43 bytes View Download

**poc.js**
617 bytes View Download

Comment 3 by ajgo@google.com on Wed, Apr 28, 2021, 5:38 PM EDT Project Member

I have so far not been able to repro on Windows.

Comment 4 by sheriffbot on Thu, Apr 29, 2021, 1:02 PM EDT Project Member

**Labels:** M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

Comment 5 by sheriffbot on Thu, Apr 29, 2021, 1:38 PM EDT Project Member

**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.

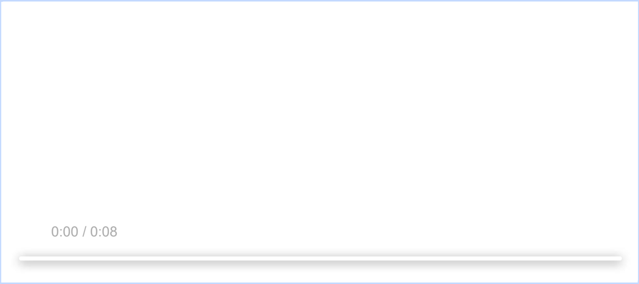
For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 6 by chrom...@gmail.com on Fri, Apr 30, 2021, 12:27 AM EDT

There is another easy way to repro this bug.

- Click on the first color indicator icon and move the tab to the right and drag it out of the tab strip then drag it back to the tab strip.

**screen.mov**
7.1 MB View Download



Comment 7 by ajgo@google.com on Fri, Apr 30, 2021, 11:27 AM EDT Project Member

**Status:** Assigned (was: Untriaged)
**Owner:** tbergquist@chromium.org
**Labels:** OS-Linux OS-Windows

Thanks - I have been able to repro on linux by changing the timeout in poc.js to 9s, waiting for the first splurge of tabs, then draging a tab left and right then in and out of the tab strip.

This is definitely on the very edge of what I would consider a security bug due to the complexity of the repro - let us know if you can repro entirely using a scripted approach.

Assigning to tbergquist based on history in browser_tab_strip_controller.cc - please reassign to someone else if they are better placed to investigate and address this security issue.

**log.asan**
28.0 KB View Download

Comment 8 by sheriffbot on Wed, May 12, 2021, 12:21 PM EDT 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 9 by tbergquist@chromium.org on Wed, May 12, 2021, 3:15 PM EDT Project Member

**Cc:** solomonkinard@chromium.org pbos@chromium.org

This one will be fixed by https://chromium-review.googlesource.com/c/chromium/src/+/2891080

Comment 10 by chrom...@gmail.com on Thu, May 13, 2021, 10:37 AM EDT

Great! so I will verify this bug once the fix is landed.

Comment 11 by solomonkinard@chromium.org on Mon, May 17, 2021, 3:51 PM EDT Project Member

crrev.com/c/2891080 merged.

Comment 12 by chrom...@gmail.com on Mon, May 17, 2021, 5:29 PM EDT

Fixed on Chromium 92.0.4511.0 (Developer Build) (x86_64) refs/heads/master@{#883573}.

Comment 13 by chrom...@gmail.com on Fri, May 21, 2021, 2:48 PM EDT

Fixed?

Comment 14 by tbergquist@chromium.org on Fri, May 21, 2021, 4:13 PM EDT Project Member

**Status:** Verified (was: Assigned)

Yes! Fixed, sorry! Thanks for verifying.

Comment 15 by sheriffbot on Sat, May 22, 2021, 12:41 PM EDT Project Member

**Labels:** reward-topanel

Comment 16 by sheriffbot on Sat, May 22, 2021, 2:00 PM EDT Project Member

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

Comment 17 by sheriffbot on Sat, May 22, 2021, 2:25 PM EDT Project Member

**Labels:** Merge-Request-92 Merge-Request-91

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M91. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to future beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M92. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

Comment 18 by sheriffbot on Sat, May 22, 2021, 2:28 PM EDT Project Member

**Labels:** -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: We are only 2 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), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 19 by sheriffbot on Sun, May 23, 2021, 2:28 PM EDT Project Member

**Labels:** -Merge-Request-92 Hotlist-Merge-Approved Merge-Approved-92

Your change meets the bar and is auto-approved for M92. Please go ahead and merge the CL to branch 4515 (refs/branch-heads/4515) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: govind@(Android), bindusuvarna@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 20 by sheriffbot on Thu, May 27, 2021, 12:16 PM EDT Project Member

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 21 by adetaylor@google.com on Thu, Jun 3, 2021, 2:22 PM EDT Project Member

**Labels:** -Merge-Review-91 Merge-Rejected-91

Rejecting merge to M91 because the fix is textually quite big (even if it's relatively simple) and as a medium severity security bug, it doesn't justify accepting any stability risk for M91. Better to release in M92... but tbergquist@ please go ahead and merge to M92.

Comment 22 by adetaylor@google.com on Thu, Jun 3, 2021, 2:29 PM EDT Project Member

**Labels:** -Merge-Approved-92 -Merge-Rejected-91 Merge-NA Release-0-M91 relnotes_update_needed

In fact, this was already merged to M91 so adjusting labels appropriately.

Comment 23 by asumaneev@google.com on Fri, Jun 4, 2021, 2:02 PM EDT Project Member

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

Marking as not applicable for LTS-86. There already was an attempt to merge the fix:
https://chromium-review.googlesource.com/c/chromium/src/+/2919770

Comment 24 by amyressler@google.com on Mon, Jun 7, 2021, 10:45 AM EDT Project Member

**Labels:** CVE-2021-30543 CVE_description-missing

Comment 25 by amyressler@chromium.org on Mon, Jun 7, 2021, 11:00 AM EDT Project Member

**Labels:** -relnotes_update_needed

rel notes updated

Comment 26 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

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

Comment 27 by asumaneev@google.com on Tue, Jun 8, 2021, 6:58 AM EDT Project Member

**Labels:** LTS-Security-90 LTS-Merge-Request-90

Comment 28 by gianluca@google.com on Wed, Jun 9, 2021, 9:08 AM EDT Project Member

**Labels:** -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 29 by amyressler@google.com on Wed, Jun 16, 2021, 6:50 PM EDT 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 30 by amyressler@chromium.org on Wed, Jun 16, 2021, 7:00 PM EDT Project Member

Congratulations, Khalil - another one! The VRP Panel has decided to award you $7,500 fro this report. Another good one!

Comment 31 by amyressler@google.com on Fri, Jun 18, 2021, 4:53 PM EDT Project Member

**Labels:** -reward-unpaid reward-inprocess

Comment 32 by rzanoni@google.com on Mon, Aug 23, 2021, 8:04 AM EDT Project Member

**Labels:** -LTS-Merge-Approved-90 LTS-Merged-90

Comment 33 by sheriffbot on Sat, Aug 28, 2021, 1:29 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