bugs chromium ▾ New issue Open issues ▾ 🔍 Search chromium issue ▾ ⚙ Sign in

☆ Starred by 4 users

Owner:	dpenning@chromium.org
CC:	🕓 desktop-pwas-team@google.com 🕓 loubrett@chromium.org 🕓 robliao@chromium.org 🕓 connily@chromium.org 🕓 markchang@chromium.org alancutter@chromium.org 🕓 top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>TabStrip>TabGroups
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	2
Type:	Bug-Security

M-100
reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-96
Target-98
Target-100
FoundIn-96
Security_Impact-Extended
Release-2-M100
CVE-2022-1313
TopChrome

Issue 1270539: heap-use-after-free in TabGroupModel::GetTabGroup

Reported by stw.s...@gmail.com on Mon, Nov 15, 2021, 6:49 PM EST

Code

VULNERABILITY DETAILS
Heap-use-after-free when a tab is added to a tab group in a tabbed PWA window.

VERSION
Chrome Version: 98.0.4703.0
Operating System: Windows 10

I found two different ways to trigger this issue. Since the stack traces point to the same function, I am reporting both of them here.

REPRODUCTION CASE #1
1. Enable #enable-desktop-pwas-tab-strip
2. Open the attached PWA and install (live: https://vuln-tabbed-pwa.websec.blog/)
3. Right-click the opened tab, select "Add tab to a new group"
4. View page source (CTRL+U)

If it crashes with "access-violation on unknown address 0xffffffffffffffff", wait 10-30s after launching Chrome.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State:

```
=================================================================
==18952==ERROR: AddressSanitizer: heap-use-after-free on address 0x12c4249caf38 at pc 0x7ffa9828f8c7 bp
0x00c42b9fd7e0 sp 0x00c42b9fd828
READ of size 8 at 0x12c4249caf38 thread T0
==18952==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ffa9828f8c6 in TabGroupModel::GetTabGroup
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_group_model.cc:43
    #1 0x7ffa95d9caec in TabStripModel::AddWebContents
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_strip_model.cc:988
    #2 0x7ffa95d830af in Navigate C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_navigator.cc:695
    #3 0x7ffa982a0c38 in chrome::AddWebContents C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_tabstrip.cc:79
    #4 0x7ffa95d7312d in Browser::AddNewContents C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser.cc:1641
    #5 0x7ffa8db808be in content::WebContentsImpl::ViewSource
C:\b\s\w\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc:5897
    #6 0x7ffa9d5f66d7 in RenderViewContextMenu::ExecuteCommand
C:\b\s\w\ir\cache\builder\src\chrome\browser\renderer_context_menu\render_view_context_menu.cc:2625
    #7 0x7ffaa0485f01 in views::MenuModelAdapter::ExecuteCommand
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_model_adapter.cc:170

    #8 0x7ffa9911141b in views::internal::MenuRunnerImpl::OnMenuClosed
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_runner_impl.cc:233
    #9 0x7ffa9d06436a in views::MenuController::ExitMenu
```

```
   #9 0x7ffa9d06426a in views::MenuController::ExitMenu
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:3175
   #10 0x7ffa9d0696b5 in views::MenuController::Accept
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:1778
   #11 0x7ffa9d068c49 in views::MenuController::OnMouseReleased
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:825
   #12 0x7ffa938189e2 in views::Widget::OnMouseEvent C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1540
   #13 0x7ffa94718ead in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:190
   #14 0x7ffa947183cd in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:139
   #15 0x7ffa94717cb7 in ui::EventDispatcherDelegate::DispatchEventToTarget
C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:83
   #16 0x7ffa947178f8 in ui::EventDispatcherDelegate::DispatchEvent
C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:55
   #17 0x7ffa991420a0 in ui::EventProcessor::OnEventFromSource
C:\b\s\w\ir\cache\builder\src\ui\events\event_processor.cc:49
   #18 0x7ffa961e0a9b in ui::EventSource::DeliverEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:117
   #19 0x7ffa961e06f5 in ui::EventSource::SendEventToSinkFromRewriter
C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:142
   #20 0x7ffa961e01f7 in ui::EventSource::SendEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:111
   #21 0x7ffa9913fa7f in views::DesktopWindowTreeHostWin::HandleMouseEvent
C:\b\s\w\ir\cache\builder\src\ui\views\widget\desktop_aura\desktop_window_tree_host_win.cc:1023
   #22 0x7ffa9d0c17d3 in views::HWNDMessageHandler::HandleMouseEventInternal
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:3146
   #23 0x7ffa9d0bac37 in views::HWNDMessageHandler::_ProcessWindowMessage
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.h:359
   #24 0x7ffa9d0ba2d6 in views::HWNDMessageHandler::OnWndProc
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:1018
   #25 0x7ffa969183d6 in gfx::WindowImpl::WndProc C:\b\s\w\ir\cache\builder\src\ui\gfx\win\window_impl.cc:306
   #26 0x7ffa96916cf1 in base::win::WrappedWindowProc<&gfx::WindowImpl::WndProc>
C:\b\s\w\ir\cache\builder\src\base\win\wrapped_window_proc.h:74
   #27 0x7ffb3aabe7e7 in CallWindowProcW+0x3f7 (C:\WINDOWS\System32\user32.dll+0x18000e7e7)
   #28 0x7ffb3aabe228 in DispatchMessageW+0x258 (C:\WINDOWS\System32\user32.dll+0x18000e228)
   #29 0x7ffa93b525ea in base::MessagePumpForUI::ProcessMessageHelper
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:542
   #30 0x7ffa93b50619 in base::MessagePumpForUI::ProcessNextWindowsMessage
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:504
   #31 0x7ffa93b4ff13 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:215
   #32 0x7ffa93b4e248 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
   #33 0x7ffa965dca65 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
   #34 0x7ffa93a25dc3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
   #35 0x7ffa8cc85aea in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
   #36 0x7ffa8cc8ae99 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
   #37 0x7ffa8cc7f487 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:49
   #38 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
   #39 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser

C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
   #40 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
```

```
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
    #41 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
    #42 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424
    #43 0x7ffa8902148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172
    #44 0x7ff716805b45 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #45 0x7ff716802c31 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #46 0x7ff716bff83f in __scrt_common_main_seh
d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #47 0x7ffb3a277033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #48 0x7ffb3c262650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x12c4249caf38 is located 8 bytes inside of 32-byte region [0x12c4249caf30,0x12c4249caf50)
freed by thread T0 here:
    #0 0x7ff7168b229b in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffa8b2e4814 in gpu::mojom::DeferredSharedImageRequest::DestroyActive
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\gpu\ipc\common\gpu_channel.mojom.cc:1962
    #2 0x7ffa8b305f37 in
std::__1::unique_ptr<gpu::mojom::DeferredSharedImageRequest,std::__1::default_delete<gpu::mojom::DeferredSharedImag
eRequest> >::reset C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\__memory\unique_ptr.h:315
    #3 0x7ffa8b2e3cb6 in gpu::mojom::DeferredRequestParams::DestroyActive
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\gpu\ipc\common\gpu_channel.mojom.cc:1716
    #4 0x7ffa8b305e61 in
std::__1::unique_ptr<gpu::mojom::DeferredRequestParams,std::__1::default_delete<gpu::mojom::DeferredRequestParams>
>::reset C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\__memory\unique_ptr.h:315
    #5 0x7ffa8b30657c in
std::__1::unique_ptr<gpu::mojom::DeferredRequest,std::__1::default_delete<gpu::mojom::DeferredRequest> >::reset
C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\__memory\unique_ptr.h:315
    #6 0x7ffa8b308f93 in
std::__1::__vector_base<mojo::StructPtr<gpu::mojom::DeferredRequest>,std::__1::allocator<mojo::StructPtr<gpu::mojom::D
eferredRequest> > >::~__vector_base C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\vector:466
    #7 0x7ffa8b2e8bae in gpu::mojom::GpuChannelProxy::FlushDeferredRequests
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\gpu\ipc\common\gpu_channel.mojom.cc:2818
    #8 0x7ffa8b7c72f6 in gpu::GpuChannelHost::InternalFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\client\gpu_channel_host.cc:155
    #9 0x7ffa8b7c70b5 in gpu::GpuChannelHost::EnsureFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\client\gpu_channel_host.cc:110
    #10 0x7ffa9d1531e5 in cc::TileManager::FlushAndIssueSignals C:\b\s\w\ir\cache\builder\src\cc\tiles\tile_manager.cc:1511
    #11 0x7ffaa04e5566 in base::internal::Invoker<base::internal::BindState<void (cc::UniqueNotifier::*)
(),base::WeakPtr<cc::UniqueNotifier> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:750
    #12 0x7ffa93aa5d54 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:157
    #13 0x7ffa965db395 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #14 0x7ffa965daa68 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #15 0x7ffa93b4ffb6 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #16 0x7ffa93b4e248 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #17 0x7ffa965dca65 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468

    #18 0x7ffa93a25dc3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
    #19 0x7ffa8cc85aea in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
```

```
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
   #20 0x7ffa8cc8ae99 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
   #21 0x7ffa8cc7f487 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:49
   #22 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
   #23 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
   #24 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
   #25 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
   #26 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424
   #27 0x7ffa8902148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172

previously allocated by thread T19 here:
   #0 0x7ff7168b239b in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
   #1 0x7ffaa63f4862 in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
   #2 0x7ffa8b7d47b6 in mojo::StructPtr<gpu::mojom::UpdateSharedImageParams>::StructPtr<const gpu::Mailbox
&,unsigned int &,gfx::GpuFenceHandle> C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\struct_ptr.h:63
   #3 0x7ffa8b7d2833 in gpu::SharedImageInterfaceProxy::UpdateSharedImage
C:\b\s\w\ir\cache\builder\src\gpu\ipc\client\shared_image_interface_proxy.cc:327
   #4 0x7ffa8b7d2504 in gpu::SharedImageInterfaceProxy::UpdateSharedImage
C:\b\s\w\ir\cache\builder\src\gpu\ipc\client\shared_image_interface_proxy.cc:306
   #5 0x7ffa9d20a1e0 in cc::OneCopyRasterBufferProvider::CopyOnWorkerThread
C:\b\s\w\ir\cache\builder\src\cc\raster\one_copy_raster_buffer_provider.cc:412
   #6 0x7ffa9d208849 in cc::OneCopyRasterBufferProvider::PlaybackAndCopyOnWorkerThread
C:\b\s\w\ir\cache\builder\src\cc\raster\one_copy_raster_buffer_provider.cc:300
   #7 0x7ffa9d2084a6 in cc::OneCopyRasterBufferProvider::RasterBufferImpl::Playback
C:\b\s\w\ir\cache\builder\src\cc\raster\one_copy_raster_buffer_provider.cc:128
   #8 0x7ffa9d16cf46 in cc::`anonymous namespace'::RasterTaskImpl::RunOnWorkerThread
C:\b\s\w\ir\cache\builder\src\cc\tiles\tile_manager.cc:132
   #9 0x7ffa94d42c92 in cc::SingleThreadTaskGraphRunner::RunTaskWithLockAcquired
C:\b\s\w\ir\cache\builder\src\cc\raster\single_thread_task_graph_runner.cc:158
   #10 0x7ffa94d428f7 in cc::SingleThreadTaskGraphRunner::Run
C:\b\s\w\ir\cache\builder\src\cc\raster\single_thread_task_graph_runner.cc:118
   #11 0x7ffa93b7156f in base::`anonymous namespace'::ThreadFunc
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:121
   #12 0x7ff7168bd843 in __asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:278
   #13 0x7ffb3a277033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
   #14 0x7ffb3c262650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

Thread T19 created by T0 here:
   #0 0x7ff7168be2d2 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_win.cpp:146
   #1 0x7ffa93b7094e in base::`anonymous namespace'::CreateThreadInternal
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:185
   #2 0x7ffa93aebd60 in base::SimpleThread::StartAsync C:\b\s\w\ir\cache\builder\src\base\threading\simple_thread.cc:51
   #3 0x7ffa8deb459c in content::VizProcessTransportFactory::VizProcessTransportFactory
C:\b\s\w\ir\cache\builder\src\content\browser\compositor\viz_process_transport_factory.cc:139
   #4 0x7ffa8cc83f7a in content::BrowserMainLoop::PostCreateThreadsImpl

C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1224
   #5 0x7ffa8cc83692 in content::BrowserMainLoop::PostCreateThreads
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:934
```

```
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:934
    #6 0x7ffa8daa8ce9 in content::StartupTaskRunner::RunAllTasksNow
C:\b\s\w\ir\cache\builder\src\content\browser\startup_task_runner.cc:43
    #7 0x7ffa8cc82d35 in content::BrowserMainLoop::CreateStartupTasks
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:859
    #8 0x7ffa8cc8a31a in content::BrowserMainRunnerImpl::Initialize
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:132
    #9 0x7ffa8cc7f434 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:45
    #10 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
    #11 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
    #12 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
    #13 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
    #14 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424
    #15 0x7ffa8902148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172
    #16 0x7ff716805b45 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #17 0x7ff716802c31 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #18 0x7ff716bff83f in __scrt_common_main_seh
d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #19 0x7ffb3a277033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #20 0x7ffb3c262650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_group_model.cc:43 in TabGroupModel::GetTabGroup
Shadow bytes around the buggy address:
  0x0516a91b9590: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x0516a91b95a0: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x0516a91b95b0: fd fd fd fd fa fa 00 00 00 00 fa fa fd fd fd fd
  0x0516a91b95c0: fa fa fd fd fd fa fa fa fd fd fd fd fa fa 00 00
  0x0516a91b95d0: 00 00 fa fa fd fd fd fd fa fa 00 00 00 00 fa fa
=>0x0516a91b95e0: 00 00 00 00 fa fa fd[fd]fd fd fa fa fd fd fd fd
  0x0516a91b95f0: fa fa fd fd fd fd fa fa 00 00 00 00 fa fa 00 00
  0x0516a91b9600: 00 00 fa fa fa fa fa fa fa fa 00 00 00 00 fa fa
  0x0516a91b9610: 00 00 00 00 fa fa fd fd fd fd fa fa 00 00 00 00
  0x0516a91b9620: fa fa 00 00 00 00 fa fa fd fd fd fd fa fa 00 00
  0x0516a91b9630: 00 00 fa fa 00 00 00 00 fa fa fd fd fd fd fa fa
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
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==18952==ABORTING
```

REPRODUCTION CASE #2
1. Enable #enable-desktop-pwas-tab-strip
2. Open the attached PWA and install (live: https://vuln-tabbed-pwa.websec.blog/)
3. Right-click the opened tab, select "Add tab to a new group"
4. (Open chrome://apps/ and uninstall the PWA) OR (Click the menu in the top right of the PWA window and select Uninstall)
5. Quickly drag the *tab* in the PWA window right after uninstalling. That way it won't close even after it was uninstalled.
6. Right-click the tab group, click New tab to the right

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State:

```
=================================================================
==23732==ERROR: AddressSanitizer: heap-use-after-free on address 0x11f2124fef48 at pc 0x7ffa9828f8c7 bp
0x0015fcdfd4a0 sp 0x0015fcdfd4e8
READ of size 8 at 0x11f2124fef48 thread T0
==23732==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ffa9828f8c6 in TabGroupModel::GetTabGroup
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_group_model.cc:43
    #1 0x7ffa95d9caec in TabStripModel::AddWebContents
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_strip_model.cc:988
    #2 0x7ffa95d830af in Navigate C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_navigator.cc:695
    #3 0x7ffa982a061a in chrome::AddTabAt C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_tabstrip.cc:40
    #4 0x7ffa98241137 in chrome::BrowserTabStripModelDelegate::AddTabAt
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\browser_tab_strip_model_delegate.cc:61
    #5 0x7ffa95da5751 in TabStripModel::ExecuteContextMenuCommand
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_strip_model.cc:1329
    #6 0x7ffaa0485f01 in views::MenuModelAdapter::ExecuteCommand
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_model_adapter.cc:170
    #7 0x7ffa9911141b in views::internal::MenuRunnerImpl::OnMenuClosed
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_runner_impl.cc:233
    #8 0x7ffa9d06426a in views::MenuController::ExitMenu
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:3175
    #9 0x7ffa9d0696b5 in views::MenuController::Accept

C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:1778
    #10 0x7ffa9d068c49 in views::MenuController::OnMouseReleased
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:835
```

```
C:\b\s\w\ir\cache\builder\src\ui\views\controls\menu\menu_controller.cc:825
   #11 0x7ffa938189e2 in views::Widget::OnMouseEvent C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1540
   #12 0x7ffa94718ead in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:190
   #13 0x7ffa947183cd in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:139
   #14 0x7ffa94717cb7 in ui::EventDispatcherDelegate::DispatchEventToTarget
C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:83
   #15 0x7ffa947178f8 in ui::EventDispatcherDelegate::DispatchEvent
C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:55
   #16 0x7ffa991420a0 in ui::EventProcessor::OnEventFromSource
C:\b\s\w\ir\cache\builder\src\ui\events\event_processor.cc:49
   #17 0x7ffa961e0a9b in ui::EventSource::DeliverEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:117
   #18 0x7ffa961e06f5 in ui::EventSource::SendEventToSinkFromRewriter
C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:142
   #19 0x7ffa961e01f7 in ui::EventSource::SendEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:111
   #20 0x7ffa9913fa7f in views::DesktopWindowTreeHostWin::HandleMouseEvent
C:\b\s\w\ir\cache\builder\src\ui\views\widget\desktop_aura\desktop_window_tree_host_win.cc:1023
   #21 0x7ffa9d0c17d3 in views::HWNDMessageHandler::HandleMouseEventInternal
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:3146
   #22 0x7ffa9d0bac37 in views::HWNDMessageHandler::_ProcessWindowMessage
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.h:359
   #23 0x7ffa9d0ba2d6 in views::HWNDMessageHandler::OnWndProc
C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:1018
   #24 0x7ffa969183d6 in gfx::WindowImpl::WndProc C:\b\s\w\ir\cache\builder\src\ui\gfx\win\window_impl.cc:306
   #25 0x7ffa96916cf1 in base::win::WrappedWindowProc<&gfx::WindowImpl::WndProc>
C:\b\s\w\ir\cache\builder\src\base\win\wrapped_window_proc.h:74
   #26 0x7ffb3aabe7e7 in CallWindowProcW+0x3f7 (C:\WINDOWS\System32\user32.dll+0x18000e7e7)
   #27 0x7ffb3aabe228 in DispatchMessageW+0x258 (C:\WINDOWS\System32\user32.dll+0x18000e228)
   #28 0x7ffa93b525ea in base::MessagePumpForUI::ProcessMessageHelper
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:542
   #29 0x7ffa93b50619 in base::MessagePumpForUI::ProcessNextWindowsMessage
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:504
   #30 0x7ffa93b4ff13 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:215
   #31 0x7ffa93b4e248 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
   #32 0x7ffa965dca65 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
   #33 0x7ffa93a25dc3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
   #34 0x7ffa8cc85aea in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
   #35 0x7ffa8cc8ae99 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
   #36 0x7ffa8cc7f487 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:49
   #37 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
   #38 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
   #39 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
   #40 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
   #41 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424

   #42 0x7ffa8902148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172
   #43 0x7ff716805b45 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
   #44 0x7ff716802e31 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
```

```
    #44 0x7ff716802c31 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #45 0x7ff716bff83f in __scrt_common_main_seh
d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #46 0x7ffb3a277033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #47 0x7ffb3c262650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x11f2124fef48 is located 8 bytes inside of 32-byte region [0x11f2124fef40,0x11f2124fef60)
freed by thread T0 here:
    #0 0x7ff7168b229b in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffa8aa6d015 in viz::mojom::internal::CompositorFrameSinkClient_OnBeginFrame_Params_Data::Validate
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\services\viz\public\mojom\compositing\compositor_frame_sink.mojom-
shared.cc:410
    #2 0x7ffa93df652d in mojo::internal::ValidateRequestGeneric
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\generated_code_util.cc:98
    #3 0x7ffa8bcb9f4c in viz::mojom::CompositorFrameSinkClientRequestValidator::Accept
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\services\viz\public\mojom\compositing\compositor_frame_sink.mojom.cc:
1632
    #4 0x7ffa9671eec1 in mojo::MessageDispatcher::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:38
    #5 0x7ffa93dfbf48 in mojo::InterfaceEndpointClient::HandleIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:657
    #6 0x7ffa93e10393 in mojo::internal::MultiplexRouter::ProcessIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:1100
    #7 0x7ffa93e0f125 in mojo::internal::MultiplexRouter::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:720
    #8 0x7ffa9671f0b2 in mojo::MessageDispatcher::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #9 0x7ffa93df3635 in mojo::Connector::DispatchMessageW
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:555
    #10 0x7ffa93df5213 in mojo::Connector::ReadAllAvailableMessages
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:613
    #11 0x7ffa93e49026 in mojo::SimpleWatcher::OnHandleReady
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\system\simple_watcher.cc:278
    #12 0x7ffa93aa5d54 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:157
    #13 0x7ffa965db395 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #14 0x7ffa965daa68 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #15 0x7ffa93b4ffb6 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #16 0x7ffa93b4e248 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #17 0x7ffa965dca65 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #18 0x7ffa93a25dc3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
    #19 0x7ffa8cc85aea in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
    #20 0x7ffa8cc8ae99 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
    #21 0x7ffa8cc7f487 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:49

    #22 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
    #23 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
```

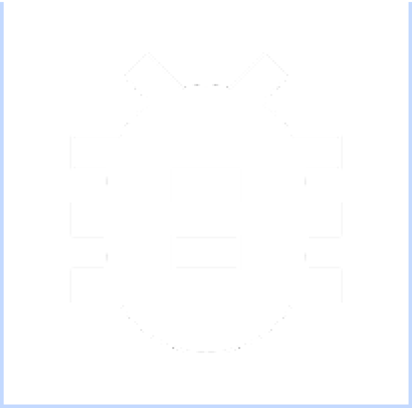
```
   #23 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
   #24 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
   #25 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
   #26 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424
   #27 0x7ffa8902148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172

previously allocated by thread T0 here:
   #0 0x7ff7168b239b in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
   #1 0x7ffaa63f4862 in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
   #2 0x7ffa8aa6cf05 in viz::mojom::internal::CompositorFrameSinkClient_OnBeginFrame_Params_Data::Validate
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\services\viz\public\mojom\compositing\compositor_frame_sink.mojom-
shared.cc:403
   #3 0x7ffa93df652d in mojo::internal::ValidateRequestGeneric
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\generated_code_util.cc:98
   #4 0x7ffa8bcb9f4c in viz::mojom::CompositorFrameSinkClientRequestValidator::Accept
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\services\viz\public\mojom\compositing\compositor_frame_sink.mojom.cc:
1632
   #5 0x7ffa9671eec1 in mojo::MessageDispatcher::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:38
   #6 0x7ffa93dfbf48 in mojo::InterfaceEndpointClient::HandleIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:657
   #7 0x7ffa93e10393 in mojo::internal::MultiplexRouter::ProcessIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:1100
   #8 0x7ffa93e0f125 in mojo::internal::MultiplexRouter::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:720
   #9 0x7ffa9671f0b2 in mojo::MessageDispatcher::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
   #10 0x7ffa93df3635 in mojo::Connector::DispatchMessageW
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:555
   #11 0x7ffa93df5213 in mojo::Connector::ReadAllAvailableMessages
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:613
   #12 0x7ffa93e49026 in mojo::SimpleWatcher::OnHandleReady
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\system\simple_watcher.cc:278
   #13 0x7ffa93aa5d54 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:157
   #14 0x7ffa965db395 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
   #15 0x7ffa965daa68 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
   #16 0x7ffa93b4ffb6 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
   #17 0x7ffa93b4e248 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
   #18 0x7ffa965dca65 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
   #19 0x7ffa93a25dc3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
   #20 0x7ffa8cc85aea in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1001
   #21 0x7ffa8cc8ae99 in content::BrowserMainRunnerImpl::Run

C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
   #22 0x7ffa8cc7f487 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:49
   #23 0x7ffa8f689d4b in content::RunBrowserProcessMain
   #23 0x7ffa8f689d4b in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
   #24 0x7ffa8f68cb9f in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1152
   #25 0x7ffa8f68bd3e in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1019
   #26 0x7ffa8f688127 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:396
   #27 0x7ffa8f689194 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:424

SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\tabs\tab_group_model.cc:43 in TabGroupModel::GetTabGroup
Shadow bytes around the buggy address:
  0x042a5489fd90: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x042a5489fda0: fd fd fd fd fa fa fd fd fd fd fa fa 00 00 00 00
  0x042a5489fdb0: fa fa fd fd fd fd fa fa 00 00 00 00 fa fa fd fd
  0x042a5489fdc0: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x042a5489fdd0: fd fd fd fd fa fa fd fd fd fd fa fa 00 00 00 00
=>0x042a5489fde0: fa fa 00 00 00 00 fa fa fd[fd]fd fd fa fa 00 00
  0x042a5489fdf0: 00 fa fa fa fd fd fd fa fa fa fd fd fd fd fa fa
  0x042a5489fe00: 00 00 00 00 fa fa fd fd fd fd fa fa fd fd fd fa
  0x042a5489fe10: fa fa fd fd fd fa fa fa fd fd fd fd fa fa 00 00
  0x042a5489fe20: 00 00 fa fa 00 00 00 00 fa fa fd fd fd fd fa fa
  0x042a5489fe30: fd fd fd fd fa fa fd fd fd fd fa fa 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
==23732==ABORTING
```

index.html
190 bytes View Download

manifest.json
380 bytes View Download

sw.js
52 bytes View Download

icon.png
3.0 KB View Download



Comment 1 by sheriffbot on Mon, Nov 15, 2021, 6:51 PM EST Project Member

Labels: external_security_report

Comment 2 by mpdenton@chromium.org on Wed, Nov 17, 2021, 1:54 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: dpenning@chromium.org
Labels: Security_Severity-Medium FoundIn-96 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-2
Components: UI>Browser>TopChrome>TabStrip>TabGroups

Thanks for the report! dpenning@ PTAL at these two bugs.

Comment 3 by sheriffbot on Wed, Nov 17, 2021, 2:01 PM EST Project Member

Labels: Security_Impact-Extended

Comment 4 by sheriffbot on Thu, Nov 18, 2021, 12:52 PM EST Project Member

Labels: Target-96 M-96

Setting milestone and target because of medium severity.

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

Comment 5 by sheriffbot on Thu, Nov 18, 2021, 1:18 PM EST 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 amyressler@google.com on Thu, Nov 18, 2021, 2:54 PM EST Project Member

Cc: pbos@chromium.org

Comment 7 by pbos@chromium.org on Thu, Nov 18, 2021, 2:55 PM EST Project Member

Cc: -pbos@chromium.org

Comment 8 by dpenning@chromium.org on Mon, Nov 22, 2021, 4:26 PM EST Project Member

Status: Started (was: Assigned)

Comment 9 by dpenning@chromium.org on Mon, Nov 22, 2021, 6:35 PM EST Project Member

Status: Assigned (was: Started)
Owner: alancutter@chromium.org
Cc: alancutter@chromium.org desktop-pwas-team@google.com
Labels: Pri-2

This feature is wholly unsupported for Apps currently.

See https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/browser.cc;l=1185?q=chrome%2Fbrowser%2Fui%2Fbrowser.cc&ss=chromium

In order to make the Tab Strip work inside of PWAs some work will need to be done to support SetTabGroupMetadata.

alancutter@ im assigning to you since you added the tab-strip flag for PWAs let me know what the next steps are here.

Im also reprioritizing this down to P2 since this is behind an experimental flag for PWAs (#enable-desktop-pwas-tab-strip)

Comment 10 by alancutter@chromium.org on Mon, Nov 22, 2021, 6:54 PM EST Project Member

Cc: dpenning@chromium.org

Comment 11 by alancutter@chromium.org on Mon, Nov 22, 2021, 7:06 PM EST Project Member

Cc: loubrett@chromium.org

We should remove this feature for PWAs as a quick fix. I'm not so familiar with the tab grouping code, is there a nice place to "turn off" the feature given a browser->type()? Could it have an enum value in Browser::WindowFeature and we use SupportsWindowFeature() to disable it for app windows?

Comment 12 by alancutter@chromium.org on Mon, Nov 22, 2021, 10:11 PM EST Project Member

This repro hits a DCHECK:

```
2021-11-23T00:00:44.535102Z FATAL chrome[940933:940933]: [browser.cc(1231)] Check failed:
!IsRelevantToAppSessionService(type_).
#0 0x7fb2f336da29 base::debug::CollectStackTrace()
#1 0x7fb2f326b913 base::debug::StackTrace::StackTrace()
#2 0x7fb2f328b073 logging::LogMessage::~LogMessage()
#3 0x7fb2f328ba5e base::internal::LoggerWithAllowedAllocations::~LoggerWithAllowedAllocations()
#4 0x5650b7e53e42 Browser::TabGroupedStateChanged()
#5 0x5650b7eae786 TabStripModel::GroupTab()
#6 0x5650b7eb15c3 TabStripModel::MoveAndSetGroup()
#7 0x5650b7eae2cd TabStripModel::MoveTabsAndSetGroupImpl()
#8 0x5650b7eaddd1 TabStripModel::AddToNewGroupImpl()
#9 0x5650b7eadb55 TabStripModel::AddToNewGroup()
#10 0x5650b7eafd95 TabStripModel::ExecuteContextMenuCommand()
```

```
bool IsRelevantToAppSessionService(Browser::Type type) {
 return (type == Browser::Type::TYPE_APP ||
         type == Browser::Type::TYPE_APP_POPUP);
}
```

Comment 13 by alancutter@chromium.org on Thu, Nov 25, 2021, 2:46 AM EST Project Member

Owner: connily@chromium.org

connily: What do you think of adding a way to disable tab groups on a per Browser basis? How complex would that change be? Would you be able to give an outline of how that might work?

Comment 14 by sheriffbot on Tue, Nov 30, 2021, 12:21 PM EST Project Member

connily: 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 15 by connily@google.com on Tue, Nov 30, 2021, 6:45 PM EST Project Member

Owner: dpenning@chromium.org
Cc: -dpenning@chromium.org connily@chromium.org

Passing to David to respond, as I think there have been some separate conversations already. Thanks!

Comment 16 by dpenning@chromium.org on Tue, Nov 30, 2021, 6:49 PM EST Project Member

Cc: markchang@chromium.org

Ill take this one back up and figure out how we want to handle disabling the TabGroups feature for arbitrary tab strips.

Comment 17 by sheriffbot on Thu, Dec 16, 2021, 12:21 PM EST Project Member

dpenning: Uh oh! This issue still open and hasn't been updated in the last 15 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 18 by alancutter@chromium.org on Mon, Dec 20, 2021, 1:30 AM EST Project Member

This is WIP: https://chromium-review.googlesource.com/c/chromium/src/+/3331181

Comment 19 by dpenning@chromium.org on Mon, Jan 3, 2022, 12:41 PM EST Project Member

Just waiting on reviews for this CL since reviewers are OOO.

Comment 20 by dpenning@chromium.org on Wed, Jan 12, 2022, 1:57 PM EST Project Member

Status: Started (was: Assigned)

Comment 21 by sheriffbot on Wed, Feb 2, 2022, 12:22 PM EST Project Member

Labels: -M-96 M-98 Target-98

Comment 22 by Git Watcher on Fri, Feb 11, 2022, 4:06 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9

commit bf9500afcb08e7dfaec3cf4f52e00618ab663ec9
Author: David Pennington <dpenning@chromium.org>
Date: Fri Feb 11 21:05:37 2022

Disable the TabGroupModel in PWAs and allow for disabling generally.

In this CL we allow for the group model to be a nullptr. the missing group model is then used to prevent a lot of the actions that occur on the tabstrip from grouping as well as disabling the option in the menu model.

~~Bug: 1270539~~
Change-Id: I3fe1dc74003dbdcb437df9fb2906d648d2ce0717
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3331181
Reviewed-by: Alan Cutter <alancutter@chromium.org>
Reviewed-by: Olivier Li <olivierli@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Reviewed-by: Ben Wells <benwells@chromium.org>
Commit-Queue: David Pennington <dpenning@chromium.org>
Cr-Commit-Position: refs/heads/main@{#970127}

[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/browser_browsertest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/tabs/existing_tab_group_sub_menu_model.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tab_groups/tab_groups_util.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/webui/tab_strip/tab_strip_ui_util.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/browser_tab_strip_model_delegate.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/sessions/session_restore.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/webui/tab_search/tab_search_page_handler.cc
[modify]

[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/webui/tab_search/tab_search_page_handler_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/views/tabs/tab_strip_browsertest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/sessions/session_service_base.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/webui/tab_strip/tab_strip_page_handler.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/browser.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/metrics/tab_stats/tab_stats_tracker_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tabs/tabs_test.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/web_applications/web_app_launch_utils.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/metrics/tab_stats/tab_stats_tracker.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/commander/entity_match.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/tabs/tab_strip_model_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/views/tabs/tab_drag_controller_interactive_uitest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/views/tabs/tab_group_editor_bubble_view_browsertest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/uma_browsing_activity_observer.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/views/tabs/tab_group_editor_bubble_view.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/tabs/tab_strip_model.h
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/commander/entity_match_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/toolbar/recent_tabs_sub_menu_model_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/browser.h
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/sessions/session_restore_browsertest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/sessions/tab_restore_browsertest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/tabs/tab_strip_model.cc

[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/browser_commands_unittest.cc

[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/browser_commands_unittest.cc
[modify]
https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/bf9500afcb08e7dfaec3cf4f52e00618ab663ec9/chrome/browser/ui/browser_finder.cc

Comment 23 by adetaylor@google.com on Thu, Mar 10, 2022, 11:27 AM EST Project Member

Cc: robliao@chromium.org

Comment 24 by sheriffbot on Wed, Mar 30, 2022, 12:22 PM EDT Project Member

Labels: -M-98 M-100 Target-100

Comment 25 by dpenning@chromium.org on Tue, Apr 5, 2022, 10:58 AM EDT Project Member

Status: Fixed (was: Started)

This is fixed, you should no longer be able to create tabs in PWAs

Comment 26 by sheriffbot on Tue, Apr 5, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 27 by sheriffbot on Tue, Apr 5, 2022, 1:41 PM EDT Project Member

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

Comment 28 by adetaylor@google.com on Mon, Apr 11, 2022, 12:58 PM EDT Project Member

Labels: Release-2-M100

Comment 29 by adetaylor@google.com on Mon, Apr 11, 2022, 1:30 PM EDT Project Member

Labels: CVE-2022-1313 CVE_description-missing

Comment 30 by amyressler@google.com on Wed, Apr 13, 2022, 7:42 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 31 by amyressler@chromium.org on Wed, Apr 13, 2022, 8:04 PM EDT Project Member

Thank you for this report, Thomas. The VRP Panel has decided to award you $3,000 for this report due to this issue not being web accessible and requiring on some non-standard workflow elements to trigger. Thank you for your efforts and reporting this issue to us!

Comment 32 by amyressler@google.com on Fri, Apr 15, 2022, 10:04 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 33 by sheriffbot on Tue, Jul 12, 2022, 1:31 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

Comment 34 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 35 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing