


[chromium](#) ▾[New issue](#)[Open issues](#) ▾[Search chromium issue](#) ▾[Sign in](#)

★ Starred by 3 users

**Owner:**[andrewxu@chromium.org](mailto:andrewxu@chromium.org)**CC:**

[rzanoni@google.com](mailto:rzanoni@google.com)  
[pbos@chromium.org](mailto:pbos@chromium.org)  
[elainechien@chromium.org](mailto:elainechien@chromium.org)  
[xiy...@chromium.org](mailto:xiy...@chromium.org)  
[skuhne@chromium.org](mailto:skuhne@chromium.org)  
 [robliao@chromium.org](mailto:robliao@chromium.org)  
[kylixrd@chromium.org](mailto:kylixrd@chromium.org)  
[msw@chromium.org](mailto:msw@chromium.org)  
[tbarzic@chromium.org](mailto:tbarzic@chromium.org)  
[ellyj...@chromium.org](mailto:ellyj...@chromium.org)  
[pkasting@chromium.org](mailto:pkasting@chromium.org)  
[mmourgos@chromium.org](mailto:mmourgos@chromium.org)

**Status:**Fixed (*Closed*)**Components:**[UI>Shell>Shelf](#)  
[Internals>Views](#)**Modified:**

Jul 29, 2022

**Backlog-Rank:**

----

**Editors:**

----

**EstimatedDays:**

----

**NextAction:**

----

**OS:**[Chrome, Lacros](#)**Pri:**

1

**Type:**[Bug-Security](#)

[Hotlist-Merge-Review](#)  
[reward-2000](#)  
[Security\\_Severity-Medium](#)  
[allpublic](#)  
[reward-inprocess](#)  
[CVE\\_description-submitted](#)  
[external\\_security\\_report](#)  
[FoundIn-100](#)  
[Security\\_Impact-Extended](#)  
[merge-merged-4664](#)  
[LTS-Merge-Merged-96](#)  
[merge-merged-4951](#)  
[merge-merged-101](#)

## Issue 1300561: Security: container-overflow in ash::ScrollableView::ShouldCountActivatedInkDrop

Reported by [chrom...@gmail.com](mailto:chrom...@gmail.com) on Thu, Feb 24, 2022, 11:07 AM EST

 Code

### VERSION

Chrome Version: 101.0.4907.0

Operating System: ChromeOS

### REPRODUCTION CASE

I repro'd this crash twice when I closed Chromium browser through the shelf context menu. I don't have specific steps to repro it constantly, but still trying to figure it out.

```
=====
==175475==ERROR: AddressSanitizer: container-overflow on address 0x6080002ca168 at pc 0x55f5a7c5a61c bp
0x7ffcc2c0b740 sp 0x7ffcc2c0b738
READ of size 8 at 0x6080002ca168 thread T0 (chrome)
==175475==WARNING: invalid path to external symbolizer!
==175475==WARNING: Failed to use and restart external symbolizer!
#0 0x55f5a7c5a61b in ViewAtBase ../../ui/views/view_model.h:83:28
#1 0x55f5a7c5a61b in view_at ../../ui/views/view_model.h:124:56
#2 0x55f5a7c5a61b in ash::ScrollableView::ShouldCountActivatedInkDrop(views::View const*) const
../../ash/shelf/scrollable_shelf_view.cc:2134:41
#3 0x55f5a7c5a3f2 in ash::ScrollableView::CreateScopedActiveInkDropCount(ash::ShelfButton const*)
../../ash/shelf/scrollable_shelf_view.cc:1018:8
#4 0x55f5a7c6f761 in ash::ShelfAppButton::SetInkDropAnimationStarted(bool) ../../ash/shelf/shelf_app_button.cc:950:48
#5 0x55f5a763797f in views::InkDrop::NotifyInkDropAnimationStarted() ../../ui/views/animation/ink_drop.cc:118:14
#6 0x55f5a73e6153 in Run ../../base/callback.h:241:12
#7 0x55f5a73e6153 in CheckAllSequencesStarted ../../ui/compositor/callback_layer_animation_observer.cc:107:33
#8 0x55f5a73e6153 in ui::CallbackLayerAnimationObserver::SetActive()
../../ui/compositor/callback_layer_animation_observer.cc:50:3
#9 0x55f5a76713d0 in views::ButtonController::OnMousePressed(ui::MouseEvent const&)
../../ui/views/controls/button/button_controller.cc:30:28
#10 0x55f5a7c6da77 in ash::ShelfAppButton::OnMousePressed(ui::MouseEvent const&)
../../ash/shelf/shelf_app_button.cc:0:0
#11 0x55f5a77bf712 in views::View::ProcessMousePressed(ui::MouseEvent const&) ../../ui/views/view.cc:3010:23
#12 0x55f5a77bf25d in views::View::OnMouseEvent(ui::MouseEvent*) ../../ui/views/view.cc:1436:11
#13 0x55f5a763ec95 in ui::ScopedTargetHandler::OnEvent(ui::Event*) ../../ui/events/scoped_target_handler.cc:28:24
#14 0x55f5a3bb45cb in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
../../ui/events/event_dispatcher.cc:190:12
#15 0x55f5a3bb3b90 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*)
../../ui/events/event_dispatcher.cc:139:5
#16 0x55f5a3bb3664 in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
../../ui/events/event_dispatcher.cc:83:14
#17 0x55f5a3bb33d0 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
../../ui/events/event_dispatcher.cc:55:15
#18 0x55f5a77dd360 in views::internal::RootView::OnMousePressed(ui::MouseEvent const&)
../../ui/views/widget/root_view.cc:418:9
#19 0x55f5a77f2d3b in views::Widget::OnMouseEvent(ui::MouseEvent*) ../../ui/views/widget/widget.cc:1520:35
#20 0x55f5a3bb45cb in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
```

```

#20 0x55f5a3bb45cd in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
./././ui/events/event_dispatcher.cc:190:12
#21 0x55f5a3bb3b90 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*)
./././ui/events/event_dispatcher.cc:139:5
#22 0x55f5a3bb3664 in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
./././ui/events/event_dispatcher.cc:83:14
#23 0x55f5a3bb33d0 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
./././ui/events/event_dispatcher.cc:55:15
#24 0x55f5a73bb0cf in ui::EventProcessor::OnEventFromSource(ui::Event*) ./././ui/events/event_processor.cc:49:17
#25 0x55f5a3bb7b9e in ui::EventSource::DeliverEventToSink(ui::Event*) ./././ui/events/event_source.cc:118:16
#26 0x55f5a3bb8096 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./././ui/events/event_source.cc:66:14
#27 0x55f5a3bb67bb in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
./././ui/events/event_rewriter.cc:88:39
#28 0x55f59796a565 in ui::EventRewriterChromeOS::RewriteMouseButtonEvent(ui::MouseEvent const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./././ui/chromeos/events/event_rewriter_chromeos.cc:1274:12
#29 0x55f59796aaa5 in ui::EventRewriterChromeOS::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./././ui/chromeos/events/event_rewriter_chromeos.cc:758:12
#30 0x55f5a3bb8046 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./././ui/events/event_source.cc:67:32
#31 0x55f5a3bb67bb in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
./././ui/events/event_rewriter.cc:88:39
#32 0x55f5a7a73f20 in ash::KeyboardDrivenEventRewriter::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./././ash/events/keyboard_driven_event_rewriter.cc:31:12
#33 0x55f5a3bb8046 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./././ui/events/event_source.cc:67:32
#34 0x55f5a3bb67bb in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
./././ui/events/event_rewriter.cc:88:39
#35 0x55f5a7a6fb94 in ash::AccessibilityEventRewriter::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./././ash/events/accessibility_event_rewriter.cc:0:0
#36 0x55f5a3bb8046 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./././ui/events/event_source.cc:67:32
#37 0x55f5a3bb67bb in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
./././ui/events/event_rewriter.cc:88:39
#38 0x55f5a787f19e in ash::Autoclick
gEventRewriter::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>)
./././ash/accessibility/autoclick/autoclick_drag_event_rewriter.cc:0:0
#39 0x55f5a3bb8046 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
./././ui/events/event_source.cc:67:32
#40 0x55f5a3bb67bb in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
./././ui/events/event_rewriter.cc:88:39
#41 0x55f5a78a2c19 in ash::FullscreenMagnifierController::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ./././ash/accessibility/magnifier/fullscreen_magnifier_controller.cc:0:0
#42 0x55f5a3bb7846 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*)
./././ui/events/event_source.cc:144:29
#43 0x55f5a7aa91c3 in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*)
./././ui/aura/window_tree_host_platform.cc:231:38
#44 0x55f5a7ab032e in ash::AshWindowTreeHostPlatform::DispatchEvent(ui::Event*)
./././ash/host/ash_window_tree_host_platform.cc:184:40
#45 0x55f5a3bc2367 in Run ./././base/callback.h:142:12
#46 0x55f5a3bc2367 in ui::DispatchEventFromNativeUiEvent(ui::Event* const&, base::OnceCallback<void (ui::Event*)>)
./././ui/events/ozone/events_ozone.cc:36:25
#47 0x55f594ebf57d in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event const&)
./././ui/ozone/platform/x11/x11_window.cc:1205:2

```

```

./././ui/ozone/platform/x11/x11_window.cc:1305:3
#48 0x55f594ebdd3 in ui::X11Window::DispatchEvent(ui::Event* const&)
./././ui/ozone/platform/x11/x11_window.cc:1258:3
#49 0x55f594ebf8ce in non-virtual thunk to ui::X11Window::DispatchEvent(ui::Event* const&)
./././ui/ozone/platform/x11/x11_window.cc:0:0
#50 0x55f5a3b787b1 in ui::PlatformEventSource::DispatchEvent(ui::Event*)
./././ui/events/platform/platform_event_source.cc:98:29
#51 0x55f5a426d033 in ui::X11EventSource::OnEvent(x11::Event const&)
./././ui/events/platform/x11/x11_event_source.cc:287:5
#52 0x55f594b0dc47 in x11::Connection::DispatchEvent(x11::Event const&) ./././ui/gfx/x/connection.cc:469:14
#53 0x55f594b0d971 in x11::Connection::ProcessNextEvent() ./././ui/gfx/x/connection.cc:520:3
#54 0x55f594b0d437 in x11::Connection::Dispatch() ./././ui/gfx/x/connection.cc:0:0
#55 0x55f594b0da22 in x11::Connection::DispatchAll() ./././ui/gfx/x/connection.cc:457:12
#56 0x55f5a1b2f8a5 in base::MessagePumpLibevent::OnLibeventNotification(int, short, void*)
./././base/message_loop/message_pump_libevent.cc:0:0
#57 0x55f5a1eaab4c in event_process_active ./././base/third_party/libevent/event.c:381:4
#58 0x55f5a1eaab4c in event_base_loop ./././base/third_party/libevent/event.c:521:4
#59 0x55f5a1b303b9 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./././base/message_loop/message_pump_libevent.cc:246:5
#60 0x55f5a19ef88a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./././base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
#61 0x55f5a192695c in base::RunLoop::Run(base::Location const&) ./././base/run_loop.cc:141:14
#62 0x55f5983b79ea in content::BrowserMainLoop::RunMainMessageLoop()
./././content/browser/browser_main_loop.cc:1073:18
#63 0x55f5983bc161 in content::BrowserMainRunnerImpl::Run()
./././content/browser/browser_main_runner_impl.cc:155:15
#64 0x55f5983b1bfa in content::BrowserMain(content::MainFunctionParams)
./././content/browser/browser_main.cc:30:28
#65 0x55f5a17046af in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*)
./././content/app/content_main_runner_impl.cc:642:10
#66 0x55f5a17071f8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./././content/app/content_main_runner_impl.cc:1175:10
#67 0x55f5a1706648 in content::ContentMainRunnerImpl::Run() ./././content/app/content_main_runner_impl.cc:1042:12
#68 0x55f5a1700e29 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./././content/app/content_main.cc:401:36
#69 0x55f5a17014a5 in content::ContentMain(content::ContentMainParams) ./././content/app/content_main.cc:429:10
#70 0x55f59376a9aa in ChromeMain ./././chrome/app/chrome_main.cc:176:12
#71 0x7feb5de700b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

```

0x6080002ca168 is located 72 bytes inside of 96-byte region [0x6080002ca120,0x6080002ca180)  
allocated by thread T0 (chrome) here:

```

#0 0x55f59376818d in operator new(unsigned long) _asan_rtl_:3
#1 0x55f5a77d68b1 in __libcpp_operator_new<unsigned long> ./././buildtools/third_party/libc++/trunk/include/new:235:10
#2 0x55f5a77d68b1 in __libcpp_allocate ./././buildtools/third_party/libc++/trunk/include/new:261:10
#3 0x55f5a77d68b1 in allocate ./././buildtools/third_party/libc++/trunk/include/__memory/allocator.h:82:38
#4 0x55f5a77d68b1 in allocate ./././buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:261:20
#5 0x55f5a77d68b1 in std::__1::__split_buffer<views::ViewModelBase::Entry,
std::__1::allocator<views::ViewModelBase::Entry>&>::__split_buffer(unsigned long, unsigned long,
std::__1::allocator<views::ViewModelBase::Entry>&) ./././buildtools/third_party/libc++/trunk/include/__split_buffer:314:29
#6 0x55f5a77d5af2 in std::__1::vector<views::ViewModelBase::Entry, std::__1::allocator<views::ViewModelBase::Entry>
>::insert(std::__1::__wrap_iter<views::ViewModelBase::Entry const*>, views::ViewModelBase::Entry const&)
./././buildtools/third_party/libc++/trunk/include/vector:1794:53
#7 0x55f5a77d65c2 in views::ViewModelBase::AddUnsafe(views::View*, int) ./././ui/views/view_model.cc:74:12
#8 0x55f5a77d65c2 in AddUnsafe ./././ui/views/view_model.cc:74:12

```

```

#8 0x55f5a7ccd911 in Add ../../ui/views/view_model.cc:121:34
#9 0x55f5a7ccd91f in ash::ShelfView::ShelfItemAdded(int) ../../ash/shelf/shelf_view.cc:2057:16
#10 0x55f5a832f1e8 in ash::ShelfModel::AddAt(int, ash::ShelfItem const&, std::__1::unique_ptr<ash::ShelfItemDelegate,
std::__1::default_delete<ash::ShelfItemDelegate> >) ../../ash/public/cpp/shelf_model.cc:159:14
#11 0x55f5ae17a65e in ChromeShelfController::InsertApplItem(std::__1::unique_ptr<ash::ShelfItemDelegate,
std::__1::default_delete<ash::ShelfItemDelegate> >, ash::ShelfItemStatus, int, ash::ShelfItemType,
std::__1::basic_string<char16_t, std::__1::char_traits<char16_t>, std::__1::allocator<char16_t> > const&)
../../chrome/browser/ui/ash/shelf/chrome_shelf_controller.cc:1371:11
#12 0x55f5ae1822cf in ChromeShelfController::EnsureAppPinnedInModelAtIndex(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, int, int)
../../chrome/browser/ui/ash/shelf/chrome_shelf_controller.cc:1308:3
#13 0x55f5ae179f22 in ChromeShelfController::UpdatePinnedAppsFromSync()
../../chrome/browser/ui/ash/shelf/chrome_shelf_controller.cc:1253:30
#14 0x55f5ae180f7c in ChromeShelfController::OnAppInstalled(content::BrowserContext*, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&)
../../chrome/browser/ui/ash/shelf/chrome_shelf_controller.cc:904:3
#15 0x55f5a884d66d in apps::AppRegistryCache::DoOnApps(std::__1::vector<mojo::StructPtr<apps::mojom::App>,
std::__1::allocator<mojo::StructPtr<apps::mojom::App> > >)
../../components/services/app_service/public/cpp/app_registry_cache.cc:153:13
#16 0x55f5a884cc12 in apps::AppRegistryCache::OnApps(std::__1::vector<mojo::StructPtr<apps::mojom::App>,
std::__1::allocator<mojo::StructPtr<apps::mojom::App> > >, apps::mojom::AppType, bool)
../../components/services/app_service/public/cpp/app_registry_cache.cc:76:3
#17 0x55f5a9717d40 in apps::AppServiceProxyBase::OnApps(std::__1::vector<mojo::StructPtr<apps::mojom::App>,
std::__1::allocator<mojo::StructPtr<apps::mojom::App> > >, apps::mojom::AppType, bool)
../../chrome/browser/apps/app_service/app_service_proxy_base.cc:674:23
#18 0x55f59722da14 in apps::mojom::SubscriberStubDispatch::Accept(apps::mojom::Subscriber*, mojo::Message*)
./gen/components/services/app_service/public/mojom/app_service.mojom.cc:5742:13
#19 0x55f5a31886ea in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
../../mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:901:54
#20 0x55f5a319b3b2 in mojo::MessageDispatcher::Accept(mojo::Message*)
../../mojo/public/cpp/bindings/lib/message_dispatcher.cc:48:24
#21 0x55f5a318b5b6 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
../../mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:658:20
#22 0x55f5a31a4e3c in
mojo::internal::MultiplexRouter::ProcessIncomingMessage(mojo::internal::MultiplexRouter::MessageWrapper*,
mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*)
../../mojo/public/cpp/bindings/lib/multiplex_router.cc:1096:42
#23 0x55f5a31a3db3 in mojo::internal::MultiplexRouter::Accept(mojo::Message*)
../../mojo/public/cpp/bindings/lib/multiplex_router.cc:716:7
#24 0x55f5a319b497 in mojo::MessageDispatcher::Accept(mojo::Message*)
../../mojo/public/cpp/bindings/lib/message_dispatcher.cc:43:19
#25 0x55f5a31805f5 in mojo::Connector::DispatchMessage(mojo::ScopedHandleBase<mojo::MessageHandle>)
../../mojo/public/cpp/bindings/lib/connector.cc:559:49
#26 0x55f5a3181e10 in mojo::Connector::ReadAllAvailableMessages()
../../mojo/public/cpp/bindings/lib/connector.cc:616:14
#27 0x55f5a316cbc6 in Run ../../base/callback.h:241:12
#28 0x55f5a316cbc6 in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&)
../../mojo/public/cpp/system/simple_watcher.cc:278:14
#29 0x55f5a19ac8e6 in Run ../../base/callback.h:142:12
#30 0x55f5a19ac8e6 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
../../base/task/common/task_annotator.cc:135:32
#31 0x55f5a19ee537 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:29)>
../../base/task/common/task_annotator.cc:74:5

```

```

./././base/task/common/task_annotator.n:74:5
#32 0x55f5a19ee537 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./././base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:385:21
#33 0x55f5a19edc37 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./././base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:290:41
#34 0x55f5a19ef1d1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./././base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
#35 0x55f5a1b2fffd in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./././base/message_loop/message_pump_libevent.cc:195:55
#36 0x55f5a19ef88a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./././base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
#37 0x55f5a192695c in base::RunLoop::Run(base::Location const&) ./././base/run_loop.cc:141:14

```

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 (/home/lbstyle/Desktop/asan-linux-release-974333/chrome+0x2234361b) (BuildId: 3ccb8d222add99c3)

Shadow bytes around the buggy address:

```

0x0c10800513d0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fa
0x0c10800513e0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd
0x0c10800513f0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fa
0x0c1080051400: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1080051410: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 fa
=>0x0c1080051420: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 [fc]fc fc
0x0c1080051430: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1080051440: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1080051450: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1080051460: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x0c1080051470: fa fa fa fa fa fa fa fa fa fa fa fa fa 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
ASan internal:        fe
Left alloca redzone:  ca
Right alloca redzone: cb

```

==175475==ABORTING

Comment 2 by [danakj@chromium.org](#) on Thu, Feb 24, 2022, 12:28 PM EST Project Member

**Summary:** Security: container-overflow in ash::ScrollableView::ShouldCountActivatedInkDrop (was: Security: Heap-use-after-free in ash::ScrollableView::ShouldCountActivatedInkDrop)

**Status:** Assigned (was: Unconfirmed)

**Owner:** skuhne@chromium.org

**Cc:** pbos@chromium.org pkasting@chromium.org msw@chromium.org tbarzic@chromium.org skuhne@chromium.org xiy...@chromium.org ellyj...@chromium.org

**Labels:** Security\_Severity-Medium OS-Chrome OS-Lacros Pri-1

**Components:** UI>Shell Internals>Views

It seems the last\_tappable\_app\_index\_ is wrong.

Can

[https://source.chromium.org/chromium/chromium/src/+main:ui/views/view\\_model.h;drc=d3a5b84f152932d25c0d42d345567c6c40bd768e;l=95](https://source.chromium.org/chromium/chromium/src/+main:ui/views/view_model.h;drc=d3a5b84f152932d25c0d42d345567c6c40bd768e;l=95) check\_index() be made into production CHECKs?

Normally critical for OOB in the browser process, but (1) we don't have a consistent repro, and (2) it's during shutdown so hard to weaponize, so I will lower the security impact to lighten the load on release TPMs.

Unable to verify a FoundIn- label since we don't have a repro, perhaps if we can root cause it.

Comment 3 by [xiy...@chromium.org](#) on Thu, Feb 24, 2022, 12:54 PM EST Project Member

**Owner:** andrewxu@chromium.org

**Components:** -UI>Shell UI>Shell>Shelf

andrewxu@, could you investigate?

Comment 4 by [adetaylor@google.com](#) on Thu, Mar 10, 2022, 11:27 AM EST Project Member

**Cc:** robliao@chromium.org

Comment 5 by [andrewxu@chromium.org](#) on Thu, Mar 10, 2022, 11:28 AM EST Project Member

**Status:** Started (was: Assigned)

On my radar now

Comment 6 by [chrom...@gmail.com](#) on Wed, Mar 16, 2022, 9:33 PM EDT

You can reproduce this with the following:

- 1) Click on 'Files' icon and Open any downloaded file
- 2) Close the opened file through the shelf context menu and try to click on 'File' icon quickly.

**screen.webm**

2.6 MB [View](#) [Download](#)





[Comment 7](#) by [chrom...@gmail.com](#) on Wed, Mar 16, 2022, 9:45 PM EDT

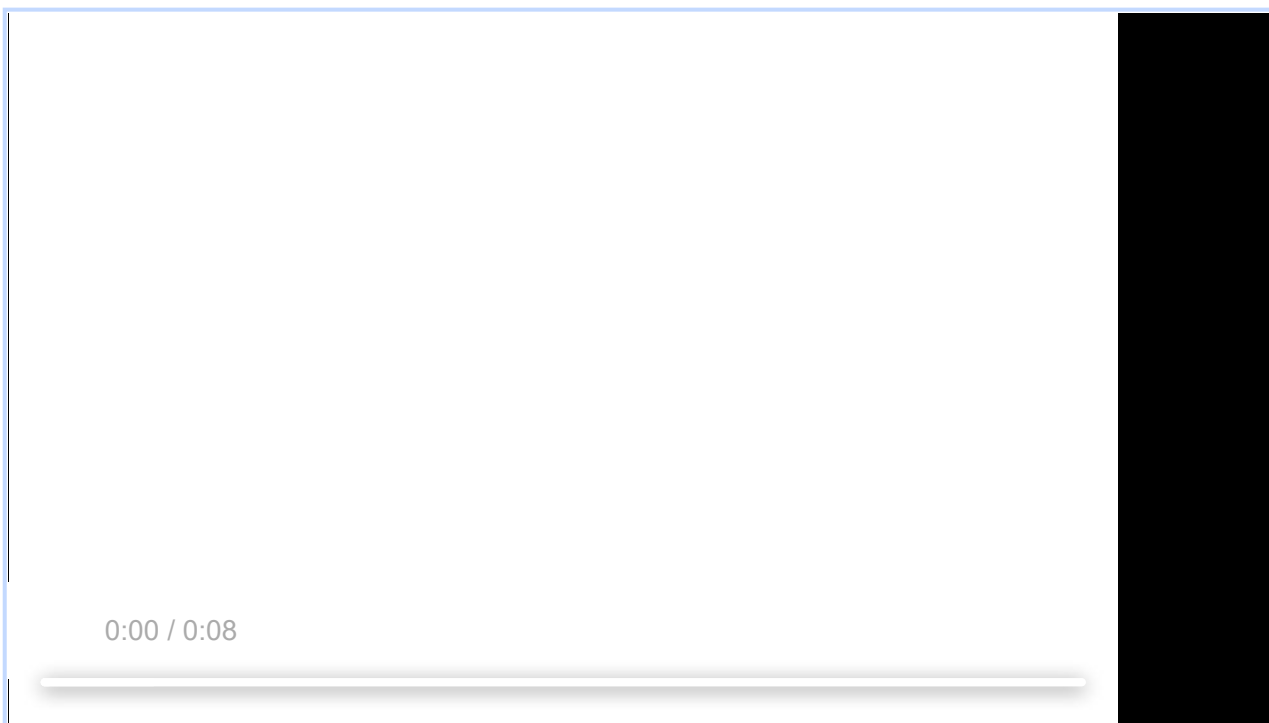
Or:

- 1) Right-click on 'chromium' icon and select 'App info'
- 2) Close the 'App info' page and try to click on 'chromium' icon quickly.

[Comment 8](#) by [chrom...@gmail.com](#) on Wed, Mar 16, 2022, 9:46 PM EDT

**screen.webm**

1.7 MB [View](#) [Download](#)



[Comment 9](#) by [adetaylor@google.com](#) on Thu, Mar 17, 2022, 11:16 AM EDT Project Member

andrewxu@ have you got as far as a root cause yet? If so, could you let us know whether this affects M98 or is a more



recent regression?

[Comment 10](#) by [andrewxu@chromium.org](#) on Thu, Mar 17, 2022, 11:36 AM EDT Project Member

Work on it right now.

[Comment 11](#) by [andrewxu@chromium.org](#) on Thu, Mar 17, 2022, 12:19 PM EDT Project Member

Reply to [comment 6](#): it is weird since I added a browser test for this scenario before [1]

I guess the cause of the bug is that: when closing an **unpinned** app through the shelf item context menu, somehow the shelf item of the app is removed before `ScrollableView::ShouldCountActivatedInkDrop()` is hit. It is why the view index is out of range. Cannot reproduce it on my Linux emulator with ASAN flag. Still investigating it.

[1]:  
[https://source.chromium.org/chromium/chromium/src/+main:chrome/browser/ui/ash/shelf/chrome\\_shelf\\_controller\\_browser\\_test.cc;l=2216;bpv=1;bpt=0;drc=91f953687242dc390ccda891d09bf7e3a04fd068](https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/ash/shelf/chrome_shelf_controller_browser_test.cc;l=2216;bpv=1;bpt=0;drc=91f953687242dc390ccda891d09bf7e3a04fd068)

[Comment 12](#) by [andrewxu@chromium.org](#) on Thu, Mar 17, 2022, 12:31 PM EDT Project Member

Good news. I can reproduce it now. Making more progress.

[Comment 13](#) by [andrewxu@chromium.org](#) on Thu, Mar 17, 2022, 12:55 PM EDT Project Member

The root cause of the bug:

Here is how `ScrollableView::last_tappable_app_index_` [1] updates when a shelf item is removed.

```
ash::ScrollableView::UpdateTappableIconIndices()
ash::ScrollableView::ViewHierarchyChanged(views::ViewHierarchyChangedDetails const&)
views::View::ViewHierarchyChangedImpl(views::ViewHierarchyChangedDetails const&)
views::View::PropagateRemoveNotifications(views::View*, views::View*, bool)
views::View::PropagateRemoveNotifications(views::View*, views::View*, bool)
views::View::DoRemoveChildView(views::View*, bool, bool, views::View*)
RemoveChildView ../../ui/views/view.cc:323:3
views::View::~View() ../../ui/views/view.cc:228:14
ash::ShelfAppButton::~ShelfAppButton() ../../ash/shelf/shelf_app_button.cc:340:35
operator() ../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
reset ../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:315:7
ash::ShelfView::FadeOutAnimationDelegate::AnimationEnded(gfx::Animation const*) ../../ash/shelf/shelf_view.cc:338:11
```

`last_tappable_app_index_` updates at the end of the fade out animation.

The crash can be reproduced by:

- (1) Add N items to shelf (N >= 2)
- (2) Remove Nth item
- (3) Before the fade out animation completes, click at N-1th item

Reply to [comment 9](#): based on the analysis, this bug should exist since the code was written. Yes, it affects M98.

[Comment 14](#) by [adetaylor@google.com](#) on Mon, Mar 21, 2022, 7:48 PM EDT Project Member

**Cc:** [kylirxd@chromium.org](#)

(auto-cc on security bug)

Comment 15 by [Git Watcher](#) on Mon, Mar 21, 2022, 9:42 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+7412ebc71d3b83b77812ebfcc5207bf482700273>

commit [7412ebc71d3b83b77812ebfcc5207bf482700273](#)

Author: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Date: Tue Mar 22 01:41:41 2022

[Shelf] Fix temporarily incorrect index value during item fade out

When a shelf item is removed, `ScrollableShelfView::last_tappable_app_index_` updates when the shelf button view is removed from the view hierarchy. However, removing view from view hierarchy is performed at the end of the fade out animation while the view is removed from the view model at the beginning of animation. This discrepancy could cause subtle issues when users interact with shelf during the fade out animation.`

Ideally, removing the view from view model should be postponed to the end of the fade out animation as well. But this change will bring the side effect that the item view to be removed is interactive during the animation. See `ShelfItemForView` used in `ShelfView::OnMenuClosed` and other places. This side effect may be hard to eliminate (for example, in ShelfView`, `view_model_` is used in many places).`

This CL performs a quick fixing by notifying `ScrollableShelfView` of shelf item removal before the fade out animation starts. Then `ScrollableShelfView` can decrease last_tappable_app_index_` instantly.`

~~Bug: 1300564~~

Change-Id: I812d919185fbac4e9447904cce6f59d54df3f476

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3532928>

Reviewed-by: Toni Barzic <[tbarzic@chromium.org](mailto:tbarzic@chromium.org)>

Commit-Queue: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Cr-Commit-Position: refs/heads/main@{#983601}

[modify] [https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable\\_shelf\\_view.h](https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable_shelf_view.h)

[modify] [https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable\\_shelf\\_view.cc](https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable_shelf_view.cc)

[modify] [https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable\\_shelf\\_view\\_unittest.cc](https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/scrollable_shelf_view_unittest.cc)

[modify] [https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/shelf\\_view.cc](https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/shelf_view.cc)

[modify] [https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/shelf\\_button\\_delegate.h](https://crrev.com/7412ebc71d3b83b77812ebfcc5207bf482700273/ash/shelf/shelf_button_delegate.h)

Comment 16 by [chrom...@gmail.com](#) on Tue, Mar 22, 2022, 2:31 PM EDT

it no longer reproduces. Fixed.

Comment 17 by [andrewxu@chromium.org](mailto:andrewxu@chromium.org) on Tue, Mar 22, 2022, 2:41 PM EDT Project Member

**Status:** Fixed (was: Started)

Comment 18 by [sheriffbot](#) on Tue, Mar 22, 2022, 2:44 PM EDT Project Member

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

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security\_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches ( as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact ([security@chromium.org](mailto:security@chromium.org)) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines:

<https://chromium.googlesource.com/chromium/src/+refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues> FoundIn guidelines:

[https://chromium.googlesource.com/chromium/src/+main/docs/security/security-labels.md#labels-relevant-for-any-type\\_bug\\_security](https://chromium.googlesource.com/chromium/src/+main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security) Thanks for your time!

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

Comment 19 by [kylixrd@chromium.org](mailto:kylixrd@chromium.org) on Mon, Mar 28, 2022, 2:31 PM EDT Project Member

Cc: [elainechien@chromium.org](mailto:elainechien@chromium.org)

Comment 20 by [chrom...@gmail.com](mailto:chrom...@gmail.com) on Mon, Apr 4, 2022, 12:07 PM EDT

Friendly ping :)

Comment 21 by [adetaylor@google.com](mailto:adetaylor@google.com) on Mon, Apr 4, 2022, 12:17 PM EDT Project Member

Status: Fixed (was: Assigned)

Labels: FoundIn-100

[andrewxu@](mailto:andrewxu@) confirms that this bug has existed since M100 and likely much before, so labelling up to keep the bots happy.

Comment 22 by [sheriffbot](#) on Mon, Apr 4, 2022, 12:23 PM EDT Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security\_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches ( as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact ([security@chromium.org](mailto:security@chromium.org)) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines:

<https://chromium.googlesource.com/chromium/src/+refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues> FoundIn guidelines:

[https://chromium.googlesource.com/chromium/src/+main/docs/security/security-labels.md#labels-relevant-for-any-type\\_bug\\_security](https://chromium.googlesource.com/chromium/src/+main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security) Thanks for your time!

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

Comment 23 by [sheriffbot](#) on Mon, Apr 4, 2022, 12:23 PM EDT Project Member

Labels: Security\_Impact-Extended

Comment 24 by [adetaylor@google.com](mailto:adetaylor@google.com) on Mon, Apr 4, 2022, 12:32 PM EDT Project Member

Status: Fixed (was: Assigned)

Gah, [#c22](#) is a known sheriffbot bug. This might just have annoyed me enough to fix it this time round...

Comment 25 by [sheriffbot](#) on Mon, Apr 4, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 26 by [sheriffbot](#) on Mon, Apr 4, 2022, 1:40 PM EDT Project Member

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

[Comment 27](#) by [amyressler@chromium.org](#) on Mon, Apr 11, 2022, 6:50 PM EDT Project Member

**Labels:** Merge-Request-101

the fix commit does not appear to have made it into 101 so manually adding merge-request label as the bot is sleeping on the job when it comes to some medium severity bugs

[Comment 28](#) by [sheriffbot](#) on Mon, Apr 11, 2022, 8:16 PM EDT Project Member

**Labels:** -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:

1. Why does your merge fit within the merge criteria for these milestones?
  - Chrome Browser: <https://chromiumdash.appspot.com/branches>
  - Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?  
<https://goto.google.com/cros-engprodcomponents>
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.

Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

[Comment 29](#) by [andrewxu@chromium.org](#) on Mon, Apr 11, 2022, 8:32 PM EDT Project Member

If I understand [comment 27](#) correctly, adding the label seems to bypass some mechanism of the bot? But I still would like to make it clear that the fixing CL should not be merged back into 101.

[Comment 30](#) by [andrewxu@chromium.org](#) on Tue, Apr 12, 2022, 12:25 PM EDT Project Member

Just talked with amyressler@ offline. My reasoning for [comment 29](#) is: this issue existed for a long time (maybe one year) before fixing so I thought it is not worthwhile to merge the fixing back. But there is the policy to fix the security bug regardless how long the bug has existed. Therefore I agree to merge the fixing back into 101 now

[Comment 31](#) by [amyressler@chromium.org](#) on Tue, Apr 12, 2022, 1:46 PM EDT Project Member

**Labels:** -Merge-Review-101 Merge-Approved-101

thank you Andrew, as this is consistent with the merge review triage process for security bugs [1] also based on that conversation, this appears to be indeed safe to merge, so approving for merge to M101, please merge to branch 4951 at your earliest availability to do so.

[1] [https://chromium.googlesource.com/chromium/src/+HEAD/docs/process/merge\\_request.md#Security-merge-triage](https://chromium.googlesource.com/chromium/src/+HEAD/docs/process/merge_request.md#Security-merge-triage)

[Comment 32](#) by [Git Watcher](#) on Tue, Apr 12, 2022, 5:59 PM EDT Project Member

**Labels:** -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773>

commit [df6fec5fdb03df9e6cfcf2e6eb522ac70b885773](#)

Author: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Date: Tue Apr 12 21:58:03 2022

[Merge to M-101][Shelf] Fix temporarily incorrect index value during item fade out

When a shelf item is removed, `ScrollableShelfView::last_tappable_app_index_` updates when the shelf button view is removed from the view hierarchy. However, removing view from view hierarchy is performed at the end of the fade out animation while the view is removed from the view model at the beginning of animation. This discrepancy could cause subtle issues when users interact with shelf during the fade out animation.`

Ideally, removing the view from view model should be postponed to the end of the fade out animation as well. But this change will bring the side effect that the item view to be removed is interactive during the animation. See `ShelfItemForView` used in ShelfView::OnMenuClosed` and other places. This side effect may be hard to eliminate (for example, in ShelfView`, view_model_` is used in many places).`

This CL performs a quick fixing by notifying `ScrollableShelfView` of shelf item removal before the fade out animation starts. Then ScrollableShelfView` can decrease last_tappable_app_index_` instantly.`

(cherry picked from commit [7412ebc71d3b83b77812ebfcc5207bf482700273](#))

~~Bug-1300561~~

Change-Id: I812d919185fbac4e9447904cce6f59d54df3f476

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+/3532928>

Reviewed-by: Toni Barzic <[tbarzic@chromium.org](mailto:tbarzic@chromium.org)>

Commit-Queue: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Cr-Original-Commit-Position: refs/heads/main@{#983601}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+/3584271>

Cr-Commit-Position: refs/branch-heads/4951@{#705}

Cr-Branched-From: [27de6227ca357da0d57ae2c7b18da170c4651438](#)-refs/heads/main@{#982481}

[modify] [https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable\\_shelf\\_view.h](https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable_shelf_view.h)

[modify] [https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable\\_shelf\\_view.cc](https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable_shelf_view.cc)

[modify] [https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/shelf\\_view.cc](https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/shelf_view.cc)

[modify] [https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable\\_shelf\\_view\\_unittest.cc](https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/scrollable_shelf_view_unittest.cc)

[modify] [https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/shelf\\_button\\_delegate.h](https://crrev.com/df6fec5fdb03df9e6cfcf2e6eb522ac70b885773/ash/shelf/shelf_button_delegate.h)

Comment 33 by [amyressler@google.com](mailto:amyressler@google.com) on Thu, Apr 21, 2022, 8:40 PM EDT Project Member

**Labels:** -reward-topanel reward-unpaid reward-2000

\*\*\* 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

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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

**Comment 34** by [amyressler@chromium.org](mailto:amyressler@chromium.org) on Thu, Apr 21, 2022, 9:44 PM EDT Project Member

Congratulations, Khalil! The VRP Panel has decided to award you \$2,000 for this report. While this issue does result in browser process memory corruption, it is significantly mitigated by user interaction and its reliance on ash shutdown to trigger, providing limited attacker control and much lower exploitability potential. We appreciate your efforts and reporting this issue to us!

**Comment 35** by [amyressler@google.com](mailto:amyressler@google.com) on Mon, Apr 25, 2022, 4:26 PM EDT Project Member

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

**Comment 36** by [amyressler@chromium.org](mailto:amyressler@chromium.org) on Mon, Apr 25, 2022, 8:38 PM EDT Project Member

**Labels:** Release-0-M101

**Comment 37** by [amyressler@google.com](mailto:amyressler@google.com) on Tue, Apr 26, 2022, 4:31 PM EDT Project Member

**Labels:** CVE-2022-1489 CVE\_description-missing

**Comment 38** by [gmpritchard@google.com](mailto:gmpritchard@google.com) on Mon, May 2, 2022, 1:45 PM EDT Project Member

**Labels:** LTS-Merge-Candidate

**Comment 39** by [rzanoni@google.com](mailto:rzanoni@google.com) on Tue, May 3, 2022, 9:16 AM EDT Project Member

**Cc:** rzanoni@google.com

**Labels:** LTS-Evaluating-96

**Comment 40** by [rzanoni@google.com](mailto:rzanoni@google.com) on Tue, May 3, 2022, 12:46 PM EDT Project Member

**Labels:** -LTS-Evaluating-96 LTS-Merge-Request-96

**Comment 41** by [sheriffbot](#) on Tue, May 3, 2022, 12:46 PM EDT Project Member

**Labels:** -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

**Comment 42** by [rzanoni@google.com](mailto:rzanoni@google.com) on Tue, May 3, 2022, 12:52 PM EDT Project Member

1. Just <https://crrev.com/c/3623278>

2. Low, no conflicts
3. 101
4. Yes

[Comment 43](#) by [gmpritchard@google.com](mailto:gmpritchard@google.com) on Mon, May 9, 2022, 11:03 AM EDT Project Member

**Labels:** -LTS-Merge-Candidate -LTS-Merge-Review-96 LTS-Merge-Approved-96

[Comment 44](#) by [Git Watcher](#) on Mon, May 9, 2022, 4:25 PM EDT Project Member

**Labels:** merge-merged-4664

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+1e0398484250809563aa782c9c5c2dbc2abe7252>

commit [1e0398484250809563aa782c9c5c2dbc2abe7252](#)

Author: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Date: Mon May 09 20:24:33 2022

[M96-LTS][Shelf] Fix temporarily incorrect index value during item fade out

When a shelf item is removed, `ScrollableShelfView::last_tappable_app_index_` updates when the shelf button view is removed from the view hierarchy. However, removing view from view hierarchy is performed at the end of the fade out animation while the view is removed from the view model at the beginning of animation. This discrepancy could cause subtle issues when users interact with shelf during the fade out animation.`

Ideally, removing the view from view model should be postponed to the end of the fade out animation as well. But this change will bring the side effect that the item view to be removed is interactive during the animation. See `ShelfItemForView` used in ShelfView::OnMenuClosed` and other places. This side effect may be hard to eliminate (for example, in ShelfView`, view_model_` is used in many places).`

This CL performs a quick fixing by notifying `ScrollableShelfView` of shelf item removal before the fade out animation starts. Then ScrollableShelfView` can decrease last_tappable_app_index_` instantly.`

(cherry picked from commit [7412ebc71d3b83b77812ebfcc5207bf482700273](#))

~~[Bug-1300561](#)~~

Change-Id: I812d919185fbac4e9447904cce6f59d54df3f476

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3532928>

Commit-Queue: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Cr-Original-Commit-Position: refs/heads/main@{#983601}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3623278>

Commit-Queue: Roger Felipe Zandoni da Silva <[rzanoni@google.com](mailto:rzanoni@google.com)>

Auto-Submit: Roger Felipe Zandoni da Silva <[rzanoni@google.com](mailto:rzanoni@google.com)>

Owners-Override: Oleh Lamzin <[lamzin@google.com](mailto:lamzin@google.com)>

Reviewed-by: Andrew Xu <[andrewxu@chromium.org](mailto:andrewxu@chromium.org)>

Reviewed-by: Oleh Lamzin <[lamzin@google.com](mailto:lamzin@google.com)>

Cr-Commit-Position: refs/branch-heads/4664@{#1628}

Cr-Branched-From: [24d41a75e01e30d300d42e0e364270e160272e7](#) refs/heads/main@{#000510}



Cr-Branched-From: [24dc4ee/5e01a29d390d43c9c2b43/2a1b92/3a/-refs/heads/main@{#929512}](#)

[modify] [https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable\\_shelf\\_view.h](https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable_shelf_view.h)

[modify] [https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable\\_shelf\\_view.cc](https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable_shelf_view.cc)

[modify] [https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/shelf\\_view.cc](https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/shelf_view.cc)

[modify] [https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable\\_shelf\\_view\\_unittest.cc](https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/scrollable_shelf_view_unittest.cc)

[modify] [https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/shelf\\_button\\_delegate.h](https://crrev.com/1e0398484250809563aa782c9c5c2dbc2abe7252/ash/shelf/shelf_button_delegate.h)

**Comment 45** by [rzanoni@google.com](#) on Mon, May 9, 2022, 4:28 PM EDT Project Member

**Labels:** -LTS-Merge-Approved-96 LTS-Merge-Merged-96

**Comment 46** 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 47** by [amyressler@google.com](#) on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

**Labels:** CVE\_description-submitted -CVE\_description-missing

**Comment 48** by [amyressler@chromium.org](#) on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

**Labels:** -CVE\_description-missing --CVE\_description-missing