bugs chromium New issue Open issues Search chromium issue Sign in

☆ Starred by 2 users

Owner:	zxdan@chromium.org
CC:	x...@chromium.org rzanoni@google.com ceb@google.com afakhry@chromium.org allenwebb@google.com
Status:	Fixed *(Closed)*
Components:	UI>Shell UI>Shell>WindowManager>Splitscreen
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-97
external_security_report
M-98
reward-7000
Target-98
FoundIn-97
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
LTS-Merge-Merged-96
Merge-Review-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100

Release-1-M99
CVE-2022-0974

Issue 1291986: Security heap-use-after-free ash/wm/splitview/split_view_divider.cc (chromeOS)

Reported by rheza...@gmail.com on Fri, Jan 28, 2022, 8:50 AM EST

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36

Steps to reproduce the problem:
I will post PoC and video on next comment

What is the expected behavior?
Not Crash

What went wrong?

```
=================================================================
==19662==ERROR: AddressSanitizer: heap-use-after-free on address 0x615000123b10 at pc 0x5562a895ac8f bp
0x7ffe7bd8cce0 sp 0x7ffe7bd8ccd8
READ of size 8 at 0x615000123b10 thread T0 (chrome)
    #0 0x5562a895ac8e in begin buildtools/third_party/libc++/trunk/include/vector:1518:30
    #1 0x5562a895ac8e in begin<std::__1::vector<base::internal::CheckedObserverAdapter,
std::__1::allocator<base::internal::CheckedObserverAdapter> > &> base/ranges/ranges.h:44:37
    #2 0x5562a895ac8e in begin<std::__1::vector<base::internal::CheckedObserverAdapter,
std::__1::allocator<base::internal::CheckedObserverAdapter> > &> base/ranges/ranges.h:105:10
    #3 0x5562a895ac8e in find_if<std::__1::vector<base::internal::CheckedObserverAdapter,
std::__1::allocator<base::internal::CheckedObserverAdapter> > &, (lambda at ../../base/observer_list.h:285:21),
base::identity, std::__1::random_access_iterator_tag> base/ranges/algorithm.h:483:26
    #4 0x5562a895ac8e in base::ObserverList<aura::WindowObserver, true, true,
base::internal::CheckedObserverAdapter>::RemoveObserver(aura::WindowObserver const*) base/observer_list.h:284:21
    #5 0x5562a97c3a0c in ash::SplitViewDivider::~SplitViewDivider() ash/wm/splitview/split_view_divider.cc:272:13
    #6 0x5562a97c3baf in ash::SplitViewDivider::~SplitViewDivider() ash/wm/splitview/split_view_divider.cc:267:39
    #7 0x5562a97afb2d in operator() buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
    #8 0x5562a97afb2d in reset buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:315:7
    #9 0x5562a97afb2d in ash::SplitViewController::EndSplitView(ash::SplitViewController::EndReason)
ash/wm/splitview/split_view_controller.cc:1315:23
    #10 0x5562a97b7670 in ash::SplitViewController::OnWindowDragStarted(aura::Window*)
ash/wm/splitview/split_view_controller.cc:1401:5
    #11 0x5562a924c6d2 in ash::DragWindowFromShelfController::OnDragStarted(gfx::PointF const&)
ash/shelf/drag_window_from_shelf_controller.cc:391:26
    #12 0x5562a924c25a in ash::DragWindowFromShelfController::DragWindowFromShelfController(aura::Window*,
gfx::PointF const&) ash/shelf/drag_window_from_shelf_controller.cc:159:3
    #13 0x5562a9245b85 in make_unique<ash::DragWindowFromShelfController, aura::Window *&, const gfx::PointF &>
buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:725:32
    #14 0x5562a9245b85 in ash::ShelfLayoutManager::MaybeStartDragWindowFromShelf(ui::LocatedEvent const&,
gfx::Vector2dF const&) ash/shelf/shelf_layout_manager.cc:2776:29
    #15 0x5562a9245e10 in ash::ShelfLayoutManager::MaybeUpdateWindowDrag(ui::LocatedEvent const&, gfx::Vector2dF
const&) ash/shelf/shelf_layout_manager.cc:2785:8
    #16 0x5562a9244e4a in ash::ShelfLayoutManager::UpdateDrag(ui::LocatedEvent const&, float, float)
ash/shelf/shelf_layout_manager.cc:2476:5

    #17 0x5562a923c931 in ash::ShelfLayoutManager::UpdateGestureDrag(ui::GestureEvent const&)
ash/shelf/shelf_layout_manager.cc:2221:3
    #18 0x5562a923b0ca in ash::ShelfLayoutManager::ProcessGestureEvent(ui::GestureEvent const&)
```

```
   #18 0x5562a923b9ce in ash::ShelfLayoutManager::ProcessGestureEvent(ui::GestureEvent const&)
ash/shelf/shelf_layout_manager.cc:758:5
   #19 0x5562a923d4d3 in ash::ShelfLayoutManager::ProcessGestureEventFromShelfWidget(ui::GestureEvent*)
ash/shelf/shelf_layout_manager.cc:811:7
   #20 0x5562a9285801 in ash::ShelfWidget::OnGestureEvent(ui::GestureEvent*) ash/shelf/shelf_widget.cc:992:27
   #21 0x5562a553994b in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*)
ui/events/event_dispatcher.cc:190:12
   #22 0x5562a5538f10 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*)
ui/events/event_dispatcher.cc:139:5
   #23 0x5562a55389e4 in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*)
ui/events/event_dispatcher.cc:83:14
   #24 0x5562a5538750 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
ui/events/event_dispatcher.cc:55:15
   #25 0x5562a896d957 in aura::WindowEventDispatcher::ProcessGestures(aura::Window*,
std::__1::vector<std::__1::unique_ptr<ui::GestureEvent, std::__1::default_delete<ui::GestureEvent> >,
std::__1::allocator<std::__1::unique_ptr<ui::GestureEvent, std::__1::default_delete<ui::GestureEvent> > > >)
ui/aura/window_event_dispatcher.cc:349:15
   #26 0x5562a8971e50 in aura::WindowEventDispatcher::PostDispatchEvent(ui::EventTarget*, ui::Event const&)
ui/aura/window_event_dispatcher.cc:584:16
   #27 0x5562a55387a4 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*)
ui/events/event_dispatcher.cc:59:15
   #28 0x5562a8976a5f in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
   #29 0x5562a553cffe in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:118:16
   #30 0x5562a553d4f6 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
ui/events/event_source.cc:66:14
   #31 0x5562a553bc1b in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
ui/events/event_rewriter.cc:88:39
   #32 0x5562990c8400 in ui::EventRewriterChromeOS::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ui/chromeos/events/event_rewriter_chromeos.cc:775:10
   #33 0x5562a553d4a6 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
ui/events/event_source.cc:67:32
   #34 0x5562a553bc1b in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
ui/events/event_rewriter.cc:88:39
   #35 0x5562a90215f0 in ash::KeyboardDrivenEventRewriter::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ash/events/keyboard_driven_event_rewriter.cc:31:12
   #36 0x5562a553d4a6 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
ui/events/event_source.cc:67:32
   #37 0x5562a553bc1b in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
ui/events/event_rewriter.cc:88:39
   #38 0x5562a901d260 in ash::AccessibilityEventRewriter::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ash/events/accessibility_event_rewriter.cc
   #39 0x5562a553d4a6 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
ui/events/event_source.cc:67:32
   #40 0x5562a553bc1b in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
ui/events/event_rewriter.cc:88:39
   #41 0x5562a8e4083e in ash::AutoclickDragEventRewriter::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ash/accessibility/autoclick/autoclick_drag_event_rewriter.cc
   #42 0x5562a553d4a6 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*)
ui/events/event_source.cc:67:32
   #43 0x5562a553bc1b in ui::EventRewriter::SendEvent(base::WeakPtr<ui::EventRewriterContinuation>, ui::Event const*)
ui/events/event_rewriter.cc:88:39

   #44 0x5562a8e211e9 in ash::FullscreenMagnifierController::RewriteEvent(ui::Event const&,
base::WeakPtr<ui::EventRewriterContinuation>) ash/accessibility/magnifier/fullscreen_magnifier_controller.cc
   #45 0x5562a553ecc6 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*)
```

```
    #45 0x5562a553cca6 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*)
ui/events/event_source.cc:144:29
    #46 0x5562a905632b in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*)
ui/aura/window_tree_host_platform.cc:231:38
    #47 0x5562a905d4be in ash::AshWindowTreeHostPlatform::DispatchEvent(ui::Event*)
ash/host/ash_window_tree_host_platform.cc:184:40
    #48 0x5562a5548377 in Run base/callback.h:142:12
    #49 0x5562a5548377 in ui::DispatchEventFromNativeUiEvent(ui::Event* const&, base::OnceCallback<void (ui::Event*)>)
ui/events/ozone/events_ozone.cc:40:25
    #50 0x5562968bc621 in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event const&)
ui/ozone/platform/x11/x11_window.cc:1304:3
    #51 0x5562968bbe77 in ui::X11Window::DispatchEvent(ui::Event* const&) ui/ozone/platform/x11/x11_window.cc:1257:3
    #52 0x5562968bc972 in non-virtual thunk to ui::X11Window::DispatchEvent(ui::Event* const&)
ui/ozone/platform/x11/x11_window.cc
    #53 0x5562a4d71f27 in ui::PlatformEventSource::DispatchEvent(ui::Event*)
ui/events/platform/platform_event_source.cc:100:29
    #54 0x5562a56363f1 in ui::X11EventSource::OnEvent(x11::Event const&)
ui/events/platform/x11/x11_event_source.cc:287:5
    #55 0x5562965e5aab in x11::Connection::DispatchEvent(x11::Event const&) ui/gfx/x/connection.cc:469:14
    #56 0x5562965e57d5 in x11::Connection::ProcessNextEvent() ui/gfx/x/connection.cc:520:3
    #57 0x5562965e529b in x11::Connection::Dispatch() ui/gfx/x/connection.cc
    #58 0x5562965e5886 in x11::Connection::DispatchAll() ui/gfx/x/connection.cc:457:12
    #59 0x5562a2fa1805 in base::MessagePumpLibevent::OnLibeventNotification(int, short, void*)
base/message_loop/message_pump_libevent.cc
    #60 0x5562a3314234 in event_process_active base/third_party/libevent/event.c:381:4
    #61 0x5562a3314234 in event_base_loop base/third_party/libevent/event.c:521:4
    #62 0x5562a2fa2319 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
base/message_loop/message_pump_libevent.cc:246:5
    #63 0x5562a2e6486a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #64 0x5562a2d9cd1c in base::RunLoop::Run(base::Location const&) base/run_loop.cc:140:14
    #65 0x556299b0592e in content::BrowserMainLoop::RunMainMessageLoop()
content/browser/browser_main_loop.cc:1053:18
    #66 0x556299b09eb5 in content::BrowserMainRunnerImpl::Run() content/browser/browser_main_runner_impl.cc:155:15
    #67 0x556299affc8a in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:30:28
    #68 0x5562a2b7ca4f in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:637:10
    #69 0x5562a2b7f551 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
content/app/content_main_runner_impl.cc:1152:10
    #70 0x5562a2b7e928 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1018:12
    #71 0x5562a2b791c4 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content/app/content_main.cc:399:36
    #72 0x5562a2b79840 in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:427:10
    #73 0x55629519153a in ChromeMain chrome/app/chrome_main.cc:176:12
    #74 0x7f21be0da0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

0x615000123b10 is located 400 bytes inside of 504-byte region [0x615000123980,0x615000123b78)
freed by thread T0 (chrome) here:
    #0 0x55629518f57d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/asan/asan_new_delete.cpp:152:3
    #1 0x5562a2e235c6 in Run base/callback.h:142:12

    #2 0x5562a2e235c6 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
base/task/common/task_annotator.cc:135:32
    #3 0x5562a2e635f3 in RunTask<(lambda at
    #3 0x5562a2e635f3 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:358:29)>
base/task/common/task_annotator.h:74:5
    #4 0x5562a2e635f3 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356:21
    #5 0x5562a2e62e42 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #6 0x5562a2e641b1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
    #7 0x5562a2fa1f5d in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
base/message_loop/message_pump_libevent.cc:195:55
    #8 0x5562a2e6486a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #9 0x5562a2d9cd1c in base::RunLoop::Run(base::Location const&) base/run_loop.cc:140:14
    #10 0x556299b0592e in content::BrowserMainLoop::RunMainMessageLoop()
content/browser/browser_main_loop.cc:1053:18
    #11 0x556299b09eb5 in content::BrowserMainRunnerImpl::Run() content/browser/browser_main_runner_impl.cc:155:15
    #12 0x556299affc8a in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:30:28
    #13 0x5562a2b7ca4f in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:637:10
    #14 0x5562a2b7f551 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
content/app/content_main_runner_impl.cc:1152:10
    #15 0x5562a2b7e928 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1018:12
    #16 0x5562a2b791c4 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content/app/content_main.cc:399:36
    #17 0x5562a2b79840 in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:427:10
    #18 0x55629519153a in ChromeMain chrome/app/chrome_main.cc:176:12
    #19 0x7f21be0da0b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 (chrome) here:
    #0 0x55629518ed1d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/asan/asan_new_delete.cpp:95:3
    #1 0x5562a8de912b in views::NativeWidgetAura::NativeWidgetAura(views::internal::NativeWidgetDelegate*)
ui/views/widget/native_widget_aura.cc:106:15
    #2 0x5562afbf9c51 in BrowserFrameAsh::BrowserFrameAsh(BrowserFrame*, BrowserView*)
chrome/browser/ui/views/frame/browser_frame_ash.cc:75:7
    #3 0x5562afbf9b32 in NativeBrowserFrameFactory::Create(BrowserFrame*, BrowserView*)
chrome/browser/ui/views/frame/native_browser_frame_factory_chromeos.cc:12:14
    #4 0x5562afb07e67 in BrowserFrame::InitBrowserFrame() chrome/browser/ui/views/frame/browser_frame.cc:91:7
    #5 0x5562afbf4791 in BrowserWindow::CreateBrowserWindow(std::__1::unique_ptr<Browser,
std::__1::default_delete<Browser> >, bool, bool) chrome/browser/ui/views/frame/browser_window_factory.cc:54:18
    #6 0x5562aef34aa2 in CreateBrowserWindow chrome/browser/ui/browser.cc:307:10
    #7 0x5562aef34aa2 in Browser::Browser(Browser::CreateParams const&) chrome/browser/ui/browser.cc:528:29
    #8 0x5562aef3373c in Browser::Create(Browser::CreateParams const&) chrome/browser/ui/browser.cc:444:14
    #9 0x5562aef80cbe in GetBrowserAndTabForDisposition chrome/browser/ui/browser_navigator.cc:268:17
    #10 0x5562aef80cbe in Navigate(NavigateParams*) chrome/browser/ui/browser_navigator.cc:578:7
    #11 0x5562aef894f9 in chrome::AddWebContents(Browser*, content::WebContents*,
std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, GURL const&,
WindowOpenDisposition, gfx::Rect const&) chrome/browser/ui/browser_tabstrip.cc:79:3

    #12 0x5562aef3f539 in non-virtual thunk to Browser::AddNewContents(content::WebContents*,
std::__1::unique_ptr<content::WebContents, std::__1::default_delete<content::WebContents> >, GURL const&,
WindowOpenDisposition, gfx::Rect const&, bool, bool*) chrome/browser/ui/browser.cc
```

```
WindowOpenDisposition, gfx::Rect const&, bool, bool*) chrome/browser/ui/browser.cc
    #13 0x55629a9f5d85 in content::WebContentsImpl::ShowCreatedWindow(content::RenderFrameHostImpl*, int,
WindowOpenDisposition, gfx::Rect const&, bool) content/browser/web_contents/web_contents_impl.cc:4068:15
    #14 0x55629a5b5bef in
content::RenderFrameHostImpl::ShowCreatedWindow(base::TokenType<blink::LocalFrameTokenTypeMarker> const&,
WindowOpenDisposition, gfx::Rect const&, bool, base::OnceCallback<void ()>)
content/browser/renderer_host/render_frame_host_impl.cc:4871:34
    #15 0x5562981bcdb7 in
blink::mojom::LocalMainFrameHostStubDispatch::AcceptWithResponder(blink::mojom::LocalMainFrameHost*,
mojo::Message*, std::__1::unique_ptr<mojo::MessageReceiverWithStatus,
std::__1::default_delete<mojo::MessageReceiverWithStatus> >)
gen/third_party/blink/public/mojom/frame/frame.mojom.cc:19012:13
    #16 0x5562a45c3c02 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:863:56
    #17 0x5562a45d6682 in mojo::MessageDispatcher::Accept(mojo::Message*)
mojo/public/cpp/bindings/lib/message_dispatcher.cc:48:24
    #18 0x5562a45c6b1a in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:658:20
    #19 0x5562a4588f05 in IPC::(anonymous
namespace)::ChannelAssociatedGroupController::AcceptOnEndpointThread(mojo::Message)
ipc/ipc_mojo_bootstrap.cc:1008:24
    #20 0x5562a4582b77 in Invoke<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>
base/bind_internal.h:543:12
    #21 0x5562a4582b77 in MakeItSo<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>
base/bind_internal.h:707:12
    #22 0x5562a4582b77 in RunImpl<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), std::__1::tuple<scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>,
mojo::Message>, 0UL, 1UL> base/bind_internal.h:780:12
    #23 0x5562a4582b77 in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous
namespace)::ChannelAssociatedGroupController::*)(mojo::Message), scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController>, mojo::Message>, void ()>::RunOnce(base::internal::BindStateBase*)
base/bind_internal.h:749:12
    #24 0x5562a2e235c6 in Run base/callback.h:142:12
    #25 0x5562a2e235c6 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
base/task/common/task_annotator.cc:135:32
    #26 0x5562a2e635f3 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:358:29)>
base/task/common/task_annotator.h:74:5
    #27 0x5562a2e635f3 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356:21
    #28 0x5562a2e62e42 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #29 0x5562a2e641b1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
    #30 0x5562a2fa1f5d in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
base/message_loop/message_pump_libevent.cc:195:55
    #31 0x5562a2e6486a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,

base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #32 0x5562a2d9cd1c in base::RunLoop::Run(base::Location const&) base/run_loop.cc:140:14
    #33 0x556299b0592c in content::BrowserMainLoop::RunMainMessageLoop()
    #33 0x556299b0592e in content::BrowserMainLoop::RunMainMessageLoop()
content/browser/browser_main_loop.cc:1053:18
    #34 0x556299b09eb5 in content::BrowserMainRunnerImpl::Run() content/browser/browser_main_runner_impl.cc:155:15
    #35 0x556299affc8a in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:30:28
    #36 0x5562a2b7ca4f in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:637:10

SUMMARY: AddressSanitizer: heap-use-after-free buildtools/third_party/libc++/trunk/include/vector:1518:30 in begin
Shadow bytes around the buggy address:
  0x0c2a8001c710: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8001c720: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8001c730: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8001c740: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2a8001c750: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c2a8001c760: fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c2a8001c770: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8001c780: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8001c790: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8001c7a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c2a8001c7b0: fa 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
==19662==ABORTING
```

Did this work before? N/A

Chrome version: 100.0.4854.0 Channel: dev
OS Version:

Comment 1 by sheriffbot on Fri, Jan 28, 2022, 8:53 AM EST   Project Member

Labels: external_security_report

Comment 2 by rheza...@gmail.com on Fri, Jan 28, 2022, 8:59 AM EST

Tested on linux-chromeOS version 100.0.4854.0
(1) pass in command line --force-tablet-mode=touch_view --touch-devices=12 --show-tabs (touch-devices=int depends on the PC, mine is 12), this command is to enable tablet mode, and no cursor

the PC, mine is 12), this command is to enable tablet mode, and no cursor.
(2) setup page close on http.server or with https://www.w3schools.com/jsref/tryit.asp?filename=tryjsref_win_close and modify the original code become

```
<!DOCTYPE html>
<html>
<body>

<h1>The Window Object</h1>
<h2>The open() and close() Methods</h2>

<button onclick="openWin()">Open "myWindow"</button>
<button onclick="closeWin()">Close "myWindow"</button>

<script>
let myWindow;

function openWin() {
  myWindow = window.open(".", ".", "width=200,height=100");
  setTimeout(function(){closeWin();},4000);
}

function closeWin() {
  myWindow.close();
}
</script>

</body>
</html>
````

(3) click run and click button "open 'myWindow'"
(4) scroll up from bottom to open split view and drag the page that being opened by "open 'myWindow' "

I will post the screen-cast soon.

Comment 3 by allenwebb@google.com on Fri, Jan 28, 2022, 5:49 PM EST Project Member

Cc: x...@chromium.org
Labels: FoundIn-97

Comment 4 by allenwebb@google.com on Fri, Jan 28, 2022, 5:50 PM EST Project Member

Cc: allenwebb@google.com
Components: UI>Shell

Comment 5 by sheriffbot on Fri, Jan 28, 2022, 5:53 PM EST Project Member

Labels: Security_Impact-Stable

Comment 6 by x...@chromium.org on Fri, Jan 28, 2022, 5:54 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: zxdan@chromium.org

Components: UI>Shell>WindowManager>Splitscreen

zxdan@, can you take a look? Thanks!

Comment 7 by rheza...@gmail.com on Fri, Jan 28, 2022, 9:52 PM EST

Hi,

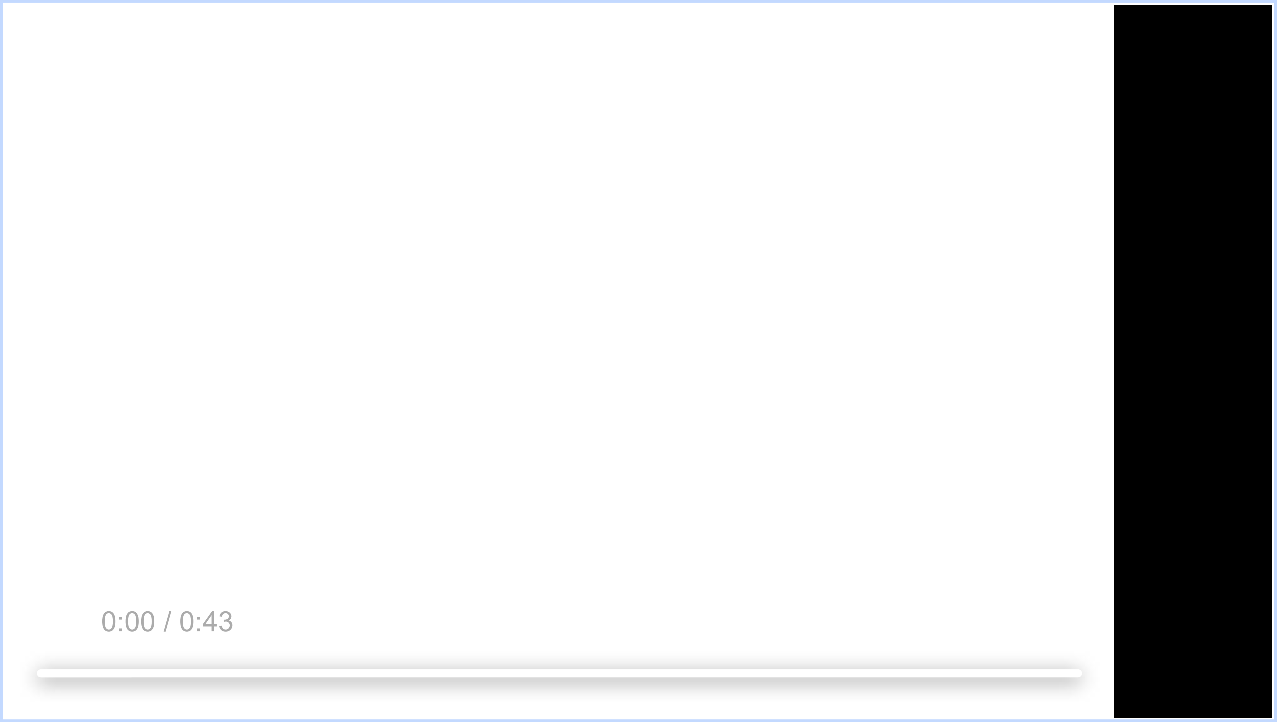
Vulnerability details:

The SplitViewController should properly reset all scoped elements, and stop observing[1] everything. This is because the shutdown may be due to the destruction of the Browser being on the splitview, so we can no longer access it. But the SplitViewController object is kept alive until splitview[2] is actually finalized.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:ash/wm/splitview/split_view_controller.cc;drc=df68b7205ea71855c06d5a0b719049fc8c49eb91;l=612
[2]
https://source.chromium.org/chromium/chromium/src/+/main:ash/wm/splitview/split_view_controller.cc;drc=df68b7205ea71855c06d5a0b719049fc8c49eb91;l=779

As promised, I uploaded the screen-cast for this issue. Please see the attachment for visibility. Thank you for looking into this issue.

screencast_1291986.webm
5.5 MB View Download



Comment 8 by allenwebb@google.com on Mon, Jan 31, 2022, 5:29 PM EST Project Member

Labels: Security_Severity-High

Comment 9 by sheriffbot on Tue, Feb 1, 2022, 12:46 PM EST Project Member

Labels: Target-97 M-97

Setting milestone and target because of high severity.

Setting milestone and target because of high severity.

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

Comment 10 by sheriffbot on Tue, Feb 1, 2022, 1:07 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. 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 11 by sheriffbot on Tue, Feb 1, 2022, 5:37 PM EST Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

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

Labels: -M-97 M-98 Target-98

Comment 13 by zxdan@chromium.org on Wed, Feb 2, 2022, 1:31 PM EST Project Member

Status: Started (was: Assigned)

Comment 14 by zxdan@chromium.org on Wed, Feb 2, 2022, 2:19 PM EST Project Member

Successfully reproduce the issue on ToT. Start to fix it.

Comment 15 by zxdan@chromium.org on Wed, Feb 2, 2022, 3:01 PM EST Project Member

The error stack I got is different. Mine should be due to destroying window while dragging:

```
#0 0x7f8249164ee9 base::debug::CollectStackTrace()
#1 0x7f82490615b3 base::debug::StackTrace::StackTrace()
#2 0x7f824907f803 logging::LogMessage::~LogMessage()
#3 0x7f824908022e base::internal::LoggerWithAllowedAllocations::~LoggerWithAllowedAllocations()
#4 0x7f824377f860 ash::SplitViewController::SnapWindow()
#5 0x7f8243782255 ash::SplitViewController::EndWindowDragImpl()
#6 0x7f82435d273c ash::DragWindowFromShelfController::OnDragEnded()
#7 0x7f82435d187a ash::DragWindowFromShelfController::CancelDrag()
#8 0x7f82435d2955 ash::DragWindowFromShelfController::OnWindowDestroying()
#9 0x7f824408d916 aura::Window::~Window()
#10 0x7f824408e052 aura::Window::~Window()
#11 0x7f82490f2d49 base::TaskAnnotator::RunTaskImpl()
#12 0x7f824911a1ea base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl()
#13 0x7f824911991b base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#14 0x7f824911a962 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#15 0x7f82492276c5 base::MessagePumpLibevent::Run()
#16 0x7f824911af0a base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run()
#17 0x7f82490c7056 base::RunLoop::Run()
#18 0x7f8241d6b7ae content::BrowserMainLoop::RunMainMessageLoop()
#19 0x7f8241d6d02f content::BrowserMainRunnerImpl::Run()
#20 0x7f8241d69079 content::BrowserMain()

#21 0x7f82425b4c66 content::RunBrowserProcessMain()
#22 0x7f82425b5fb2 content::ContentMainRunnerImpl::RunBrowser()
#23 0x7f82425b5b22 content::ContentMainRunnerImpl::Run()
```

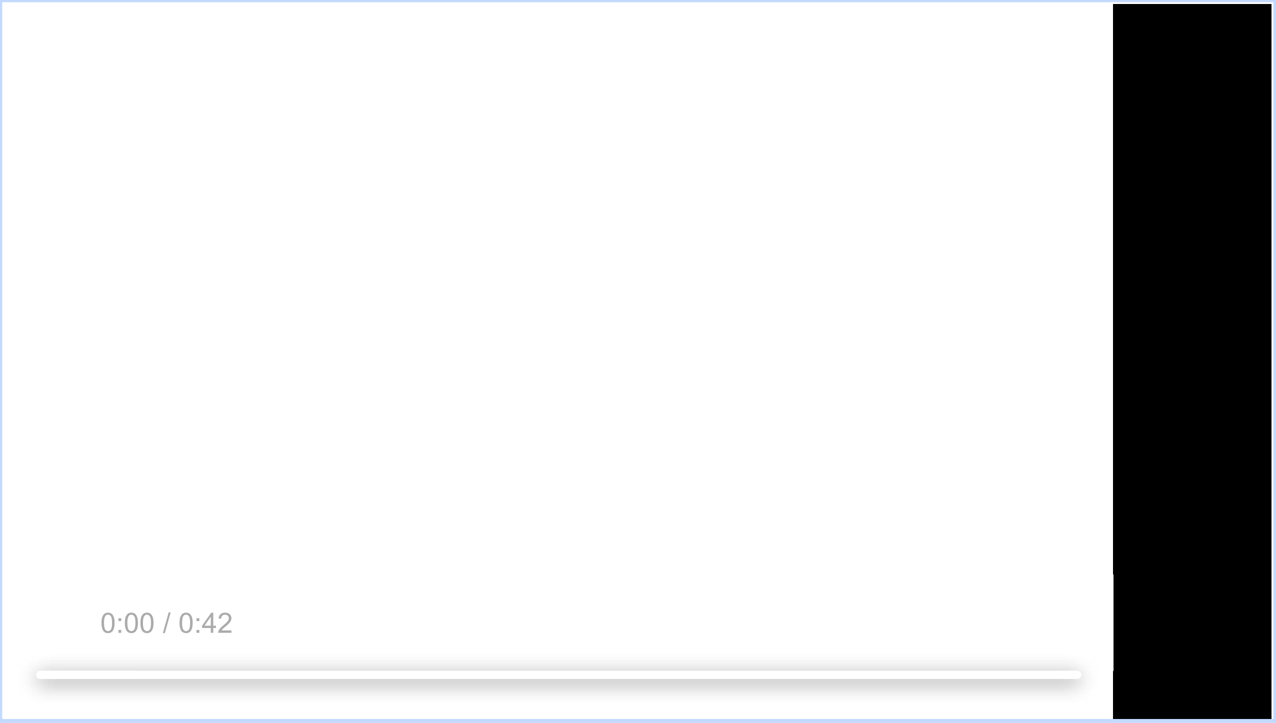
```
#23 0x7f82425b5b22 content::ContentMainRunnerImpl::Run()
#24 0x7f82425b3ccf content::RunContentProcess()
#25 0x7f82425b3db1 content::ContentMain()
#26 0x562bb21efe01 ChromeMain
#27 0x562bb21efcfe main
#28 0x7f82367d77ed __libc_start_main
#29 0x562bb21efc3a _start
Task trace:
#0 0x7f8243d86b75 views::NativeWidgetAura::Close()
#1 0x562bb4b3e06f Browser::TabStripEmpty()
#2 0x7f82473cc8c1 IPC::(anonymous namespace)::ChannelAssociatedGroupController::Accept()
#3 0x7f8248140510 mojo::SimpleWatcher::Context::Notify()
Crash keys:
  "ui_scheduler_async_stack" = "0x7F8243D86B75 0x562BB4B3E06F"
  "io_scheduler_async_stack" = "0x7F82473CCCED 0x7F8243D86B75"

Received signal 6
#0 0x7f8249164ee9 base::debug::CollectStackTrace()
#1 0x7f82490615b3 base::debug::StackTrace::StackTrace()
#2 0x7f8249164a08 base::debug::(anonymous namespace)::StackDumpSignalHandler()
#3 0x7f8236d60200 (/usr/lib/x86_64-linux-gnu/libpthread-2.33.so+0x131ff)
#4 0x7f82367ec891 gsignal
#5 0x7f82367d6536 abort
#6 0x7f8249164095 base::debug::BreakDebuggerAsyncSafe()
#7 0x7f824907fcb8 logging::LogMessage::~LogMessage()
#8 0x7f824908022e base::internal::LoggerWithAllowedAllocations::~LoggerWithAllowedAllocations()
#9 0x7f824377f860 ash::SplitViewController::SnapWindow()
#10 0x7f8243782255 ash::SplitViewController::EndWindowDragImpl()
#11 0x7f82435d273c ash::DragWindowFromShelfController::OnDragEnded()
#12 0x7f82435d187a ash::DragWindowFromShelfController::CancelDrag()
#13 0x7f82435d2955 ash::DragWindowFromShelfController::OnWindowDestroying()
#14 0x7f824408d916 aura::Window::~Window()
#15 0x7f824408e052 aura::Window::~Window()
#16 0x7f82490f2d49 base::TaskAnnotator::RunTaskImpl()
#17 0x7f824911a1ea base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl()
#18 0x7f824911991b base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#19 0x7f824911a962 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#20 0x7f82492276c5 base::MessagePumpLibevent::Run()
#21 0x7f824911af0a base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run()
#22 0x7f82490c7056 base::RunLoop::Run()
#23 0x7f8241d6b7ae content::BrowserMainLoop::RunMainMessageLoop()
#24 0x7f8241d6d02f content::BrowserMainRunnerImpl::Run()
#25 0x7f8241d69079 content::BrowserMain()
#26 0x7f82425b4c66 content::RunBrowserProcessMain()
#27 0x7f82425b5fb2 content::ContentMainRunnerImpl::RunBrowser()
#28 0x7f82425b5b22 content::ContentMainRunnerImpl::Run()
#29 0x7f82425b3ccf content::RunContentProcess()
#30 0x7f82425b3db1 content::ContentMain()
#31 0x562bb21efe01 ChromeMain
#32 0x562bb21efcfe main
#33 0x7f82367d77ed __libc_start_main

#34 0x562bb21efc3a _start
  r8: 0000000000000000  r9: 00007ffc7228a4c0 r10: 0000000000000008 r11: 0000000000000246
 r12: 0000562bbb49dd60 r13: 00000000000008f2 r14: 0000562bb93f9e30 r15: 00007ffc7228a720
 r12: 0000562bbb49dd60 r13: 00000000000008f2 r14: 0000562bb93f0e30 r15: 00007ffc7228a720
  di: 0000000000000002  si: 00007ffc7228a4c0  bp: 00007ffc7228a710  bx: 00007f8233f81fc0
  dx: 0000000000000000  ax: 0000000000000000  cx: 00007f82367ec891  sp: 00007ffc7228a4c0
  ip: 00007f82367ec891 efl: 0000000000000246 cgf: 002b000000000033 erf: 0000000000000000
 trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]
```

Comment 16 by zxdan@chromium.org on Wed, Feb 2, 2022, 3:14 PM EST Project Member

rhezashan@, allenwebb@, I tried to reproduce this issue by following the steps described in the video in comment 7. However, I only got the error stack in comment 15. Could any of you help me validate my reproduce procedure in the video attached?

I'm going to first look at the issue I found in the video. Please let me know if there is anything wrong with my reproducing steps. Thanks!

Screen recording 2022-02-02 12.09.06 PM.webm
4.7 MB View Download



Comment 17 by rheza...@gmail.com on Wed, Feb 2, 2022, 3:22 PM EST

re #c15:

I'm sorry but it look like the stack trace from your comment #c15 is less than mine. If you able to screen-cast, maybe I can figure out.

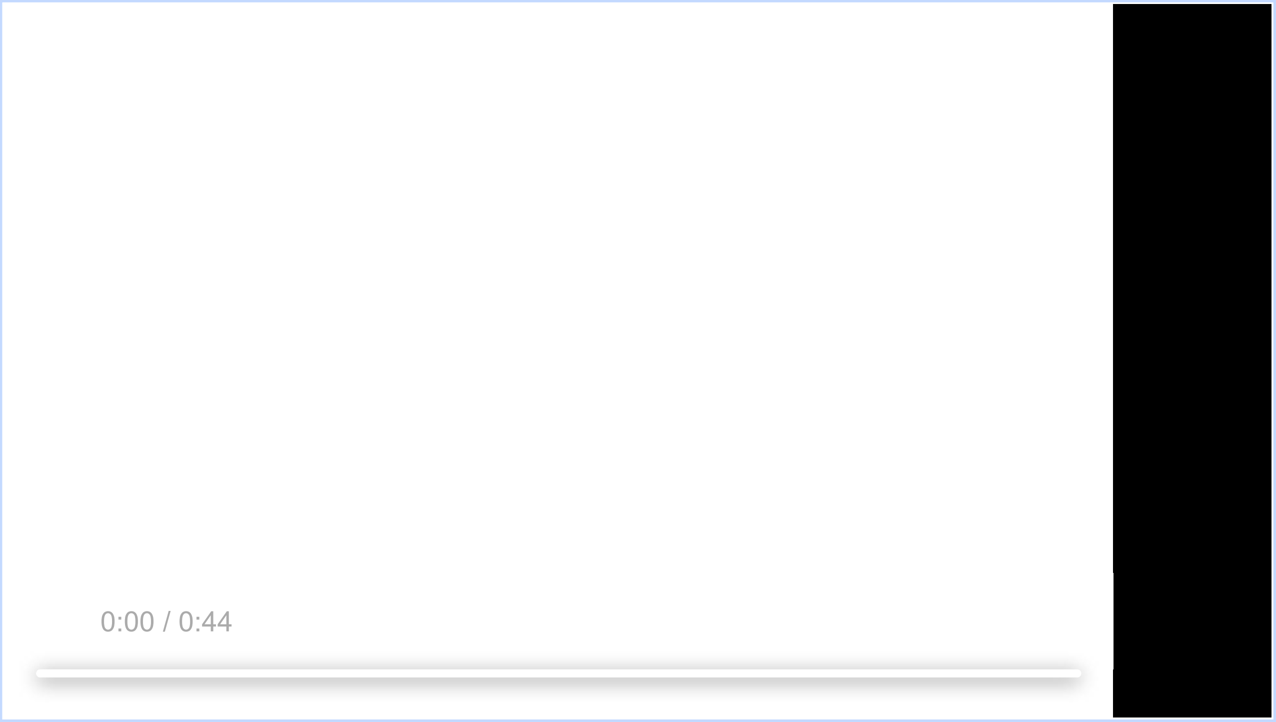
on my step:
(1) Ensure enables --force-tablet-mode=touch_view to simulate tablet mode.
(2) xinput and chose virtual slave pointer (mine 12) to active no cursor like on Chromebook tablet.
(3) Run ~/src/asan-linux-release-966287/chrome --force-tablet-mode=touch_view --touch-devices=12
(4) Open file manager and put on left side and this will active splitview.
(5) Open browser then put on right side and click `open window`.

(6) Open rhezashan.github.io/pocs/openWindow.html and then swipe from button to grab active window .

I've tested on Chromium 100.0.4867.0 (r966287 Asan prebuilt) just now and I could repro. Please see new screen cast for

I've tested on Chromium 100.0.4867.0 (r966287 Asan prebuilt) just now and I could repro. Please see new screen-cast for visibility.
Hope this helps.

screencast_1291986_b.webm
4.2 MB View Download



Comment 18 by rheza...@gmail.com on Wed, Feb 2, 2022, 3:24 PM EST

re #c16:

sorry I was typing on comment, didn't see your new comment in meantime.

Comment 19 by zxdan@chromium.org on Wed, Feb 2, 2022, 3:54 PM EST Project Member

Interesting, I was following exactly the same steps. Seems your crash also happened while dragging the destroying window.

Let me try it again. In either case, destroying a window while dragging is an issue needed to be fixed.

Comment 20 by rheza...@gmail.com on Wed, Feb 2, 2022, 3:57 PM EST

Fyi I tested on gs://chromium-browser-asan/linux-release-chromeos/asan-linux-release-966287.zip

Comment 21 by zxdan@chromium.org on Wed, Feb 2, 2022, 3:59 PM EST Project Member

Thanks, rhezashan@.

Comment 22 by zxdan@chromium.org on Wed, Feb 2, 2022, 6:15 PM EST Project Member

Cc: afakhry@chromium.org

Comment 23 by jorgelo@chromium.org on Wed, Feb 9, 2022, 12:28 PM EST Project Member

This is a P1 bug, per our SLO guidelines (https://chromium.googlesource.com/chromiumos/docs/+/HEAD/security_severity_guidelines.md#service-level-objectives) this requires updates every week. Where are we here?

this requires updates every week. Where are we here?

Comment 24 by zxdan@chromium.org on Wed, Feb 9, 2022, 1:08 PM EST Project Member

Tried on ASAN build but still cannot get the same stack trace. Fixing the crash I got to see if it is related to the current issue.

Comment 25 by rheza...@gmail.com on Wed, Feb 9, 2022, 1:32 PM EST

fyi: I ran ~/asan/chromeOS/asan-linux-release-968893/chrome --force-tablet-mode=touch_view --touch-devices=9 --ash-host-window-bounds="400+300-1600x1000" --user-data-dir=/tmp/chromeos from command line. Hope this helps.

Comment 26 by x...@chromium.org on Thu, Feb 10, 2022, 1:22 PM EST Project Member

FYI I tried on normal Chrome build and also ASAN build locally, and I can get the same crash stack as what zxdan@ got in comment#15, but not the original crash stack in the original report. I think they might have the same underlying root cause. we can try to fix this crash stack and see if it can also resolve the reported crash.

Comment 27 by zxdan@chromium.org on Thu, Feb 10, 2022, 1:24 PM EST Project Member

thanks for confirming this, xdai@! Working on this.

Comment 28 by rheza...@gmail.com on Fri, Feb 11, 2022, 3:08 PM EST

Hello

I'm sorry for this bug if you'are can not repro this issue and got different stack.
Fyi, today I tried build 2 types of ASAN locally :
(1) argn.gs

```
is_asan = true
target_os = "chromeos"
```

I can get the same crash similar comment #c15 and #c26 but my local machine didn't show the symbolized

```
=============
2022-02-11T15:47:43.076348Z FATAL chrome[1607274:1607274]: [split_view_controller.cc(819)] Check failed: window && CanSnapWindow(window).
#0 0x558dee1a9a9b (/chrome/linux-chromeOS/src/out/Default/chrome+0xfad5a9a)
#1 0x7f29ec4f618f (/chrome/linux-chromeOS/src/out/Default/libbase.so+0xd8118e)
#2 0x7f29ebdad50d (/chrome/linux-chromeOS/src/out/Default/libbase.so+0x63850c)
#3 0x7f29ebdad385 (/chrome/linux-chromeOS/src/out/Default/libbase.so+0x638384)
#4 0x7f29ebe7b951 (/chrome/linux-chromeOS/src/out/Default/libbase.so+0x706950)
...snip..
  #41 0x558dee16df4a (/chrome/linux-chromeOS/src/out/Default/chrome+0xfa99f49)
Task trace:
#0 0x7f29bace800b (/chrome/linux-chromeOS/src/out/Default/libviews.so+0xec500a)
#1 0x558e0dc04a98 (/chrome/linux-chromeOS/src/out/Default/chrome+0x2f530a97)
#2 0x7f29df064efd (/chrome/linux-chromeOS/src/out/Default/libipc.so+0x128efc)
#3 0x7f29e53f6fbc (/chrome/linux-chromeOS/src/out/Default/libmojo_public_system_cpp.so+0x75fbb)
Crash keys:
  "ui_scheduler_async_stack" = "0x7F29BACE800B 0x558E0DC04A98"
  "io_scheduler_async_stack" = "0x7F29DF065CF0 0x7F29BACE800B"

Received signal 6
#0 0x558dee1a9a9b (/chrome/linux-chromeOS/src/out/Default/chrome+0xfad5a9a)
#1 0x7f29ec4f618f (/chrome/linux-chromeOS/src/out/Default/libbase.so+0xd8118e)
#2 0x7f29ebdad50d (/chrome/linux-chromeOS/src/out/Default/libbase.so+0x63850c)
#3 0x7f29ebdad385 (/chrome/linux-chromeOS/src/out/Default/libbase.so+0x638384)
..snip
```

```
..snip...
#48 0x558dee16df4a (/chrome/linux-chromeOS/src/out/Default/chrome+0xfa99f49)
  r8: 0000000000000000  r9: 00007ffc828a2d60 r10: 0000000000000008 r11: 0000000000000246
 r12: 0000558dee16df20 r13: 00007ffc828a5b90 r14: 0000000000000000 r15: 0000000000000000
  di: 0000000000000002  si: 00007ffc828a2d60  bp: 00007ffc828a2fb0  bx: 00007f28d9dbd0c0
  dx: 0000000000000000  ax: 0000000000000000  cx: 00007f28ee49418b  sp: 00007ffc828a2d60
  ip: 00007f28ee49418b efl: 0000000000000246 cgf: 002b000000000033 erf: 0000000000000000
 trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]
Calling _exit(EXIT_FAILURE). Core file will not be generated.
```

This crash happen when I try to swipe up, after hit openWindow.html

(2) gn gen out/Default '--args=dcheck_always_on=false enable_ipc_fuzzer=true is_asan=true is_component_build=false is_debug=false is_lsan=true target_os= "chromeos" v8_enable_verify_heap=true'. This gn args I copied from prebuilt from e.q asan-linux-release-968893.zip and build them in my local pc.
I can get the same stack trace from #c0.

I was just wondering what's your gn args?

Comment 29 by zxdan@chromium.org on Fri, Feb 11, 2022, 3:12 PM EST Project Member

No worries, rhezashan@! Thanks so much for reporting this bug. I think this stack trace may be same with mine.
Here is my gn args:

```
use_goma = true        # Googlers: Use build farm, compiles faster.
goma_dir = "~/depot_tools/.cipd_bin"
target_os = "chromeos"
is_component_build = true  # Links faster.
is_debug = false           # Release build, runs faster.
is_asan = true
dcheck_always_on = true    # Enables DCHECK despite release build.
enable_nacl = false        # Skips native client build, compiles faster.
```

Comment 30 by rheza...@gmail.com on Fri, Feb 11, 2022, 3:34 PM EST

zxdan@,

Thanks for the info and for looking this issue. If you have more bandwidth, do you mind having a test with local build gn args similar to point (2) in #c28 or gn args below:

```
dcheck_always_on = on
enable_ipc_fuzzer = true
goma_dir = "~/depot_tools/.cipd_bin"
is_asan = true
is_component_build = false
is_debug = false
is_lsan = true
target_os = "chromeos"
use_goma = true
v8_enable_verify_heap = true
```

Thanks

Comment 31 by zxdan@chromium.org on Fri, Feb 11, 2022, 5:14 PM EST Project Member

Thanks for sharing your arguments. I will try it now.

Comment 32 by zxdan@chromium.org on Mon, Feb 14, 2022, 1:23 PM EST Project Member

I tried with the same gn args provided in comment 30 and run the emulator with the same arguments provided in comment 25.
I got the similar stack trace in comment 28.

```
Check failed: window && CanSnapWindow(window).
#0 0x55cf5aa328ff (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15bda8fe)
#1 0x55cf6c5cbc29 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27773c28)
#2 0x55cf6c2b11c3 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274591c2)
#3 0x55cf6c316ac6 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274beac5)
#4 0x55cf6c318a0e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274c0a0d)
#5 0x55cf73e53f52 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2effbf51)
#6 0x55cf73e5c718 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2f004717)
#7 0x55cf738101a6 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b81a5)
#8 0x55cf7380d0bf (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b50be)
#9 0x55cf7381093e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b893d)
#10 0x55cf72d613b8 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2df093b7)
#11 0x55cf72d62af2 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2df0aaf1)
#12 0x55cf6c46fa5a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27617a59)
#13 0x55cf6c4e6b5f (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768eb5e)
#14 0x55cf6c4e56be (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768d6bd)
#15 0x55cf6c4e7c42 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768fc41)
#16 0x55cf6c72dd5d (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x278d5d5c)
#17 0x55cf6c4e8a6b (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27690a6a)
#18 0x55cf6c3e3ccb (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2758bcca)
#19 0x55cf60990e54 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb38e53)
#20 0x55cf6099623a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb3e239)
#21 0x55cf6098a44b (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb3244a)
#22 0x55cf6c16243a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730a439)
#23 0x55cf6c165902 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730d901)
#24 0x55cf6c164bc1 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730cbc0)
#25 0x55cf6c15e6d8 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x273066d7)
#26 0x55cf6c15ed6e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27306d6d)
#27 0x55cf5aaac136 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15c54135)
#28 0x55cf5aaabf20 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15c53f1f)
#29 0x7f318e2a07ed (/usr/lib/x86_64-linux-gnu/libc-2.33.so+0x277ec)
#30 0x55cf5a9f91ea (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15ba11e9)
Task trace:
#0 0x55cf732e5f1b (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e48df1a)
#1 0x55cf7a59b857 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x35743856)
#2 0x55cf6deedc49 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x29095c48)
#3 0x55cf6df2016a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x290c8169)
Crash keys:
  "total-discardable-memory-allocated" = "4194304"
  "gpu-gl-renderer" = "llvmpipe (LLVM 12.0.1, 256 bits)"
  "gpu-gl-vendor" = "Mesa/X.org"
  "gpu-generation-intel" = "0"
  "gpu-vsver" = "4.50"
  "gpu-psver" = "4.50"

  "gpu-driver" = "21.2.6"
  "gpu-devid" = "0x0000"
  "gpu-venid" = "0x0000"
  "gpu-venid" = "0x0000"
  "ui_scheduler_async_stack" = "0x55CF732E5F1B 0x55CF7A59B857"
  "lacros-enabled" = "no"
  "num-extensions" = "0"
  "num-users" = "1"
  "io_scheduler_async_stack" = "0x55CF6DF2016A 0x0"
  "variations" = "6aa15a86-9d8c1aae,69d4ebd5-3f4a17df,65570806-377be55a,ade3efeb-e1cc0f14,f5a851ad-
3f4a17df,3fd33f16-fa281276,6a2df91f-6a2df91f,313957be-3ef44cd2,17b84626-3f4a17df,255dfea8-cf12f279,b7bee85d-
3f4a17df,b2a04140-3f4a17df,3482a891-410c5d63,62194d16-ffd50acc,b53f3ef9-3f4a17df,be47a367-3f4a17df,f9152fd1-
9b7fba90,ef4764d7-c9f4d4ef,a257327f-3f4a17df,34a9ddc3-54a64e37,f7a3ec9-bd336006,d3566fbd-c6f74b94,94a9c28-
6c491040,3fa8d059-3fa8d059,ad143c8a-3f4a17df,931c5f72-3f4a17df,b1ceb06f-3f4a17df,8ebcf27b-fa162b18,727723f1-
40193c20,b012722b-3f4a17df,9e5c75f1-30e1b12b,b8014e4c-3f4a17df,39ec51c3-572726d7,b125737b-
c3e62289,eddd0d82-3f4a17df,e6d63f79-3f4a17df,8d7344de-3f4a17df,a77166f2-a77166f2,90a7075b-725c8fbe,51266b12-
20b9d020,8bccc03b-3f4a17df,fc7e4d22-3f4a17df,4ea303a6-3f4a17df,3042ad4b-ad2fa222,3487aa71-84708353,4e3ec83a-
e4938e2c,ed3b6c40-f6c8ea70,1d606bb5-8d14c5d8,863ba1ea-3f4a17df,722b8030-3f4a17df,fbe267b5-
7f60b823,8470b833-3f4a17df,47d92407-5b5edf5b,4b9a5bc0-efbbc50a,a8347de-4699d86a,49a20295-
49a20295,1248751e-3f4a17df,6cbcf5b7-3f4a17df,733cb831-49b2945c,b0f15b33-b0f15b33,e79de56c-dee0823,7760b5b2-
3f4a17df,551dab91-3f4a17df,a2e38c9c-3f4a17df,8bfdd36f-3f4a17df,32d6b1fe-3f4a17df,e3969921-5cbb6de6,3673692f-
8580b57b,d051cdc0-3f4a17df,1bb6a450-3f4a17df,3e7d7783-f38a9353,9e91ce29-3f4a17df,3b96a1d-3f4a17df,248e3a0-
3f4a17df,6becb1e-a6ea97a2,dba92675-f23d1dea,5306c29b-9cbf73ff,44c2e2c0-3f4a17df,a112f012-3f4a17df,6e08fc3e-
3f4a17df,6cb5e962-3f4a17df,2ba47366-3f4a17df,83890985-5cbb6de6,2ccd0408-804b6bff,234de0a0-ace4e138,248c3fbd-
3f4a17df,ca5a2953-ff983c32,bf4029fe-1776d9e,74f8fa8f-74f8fa8f,ca51d624-3f4a17df,7c2504d0-3d47f4f4,357a64de-
dee0823,3e09e9b1-3f4a17df,730a7fb7-3f4a17df,54410569-3f4a17df,f48c01d3-6eb2bd2b,9481ce98-3d47f4f4,4b935545-
3d47f4f4,9a38bae3-3d47f4f4,c1405ec8-fb0c8ff1,122c746b-3d47f4f4,6f3a6be-3d47f4f4,d69d967d-3695c92e,"
  "num-experiments" = "103"
  "switch-2" = "--touch-devices=4"
  "switch-1" = "--force-tablet-mode=touch_view"
  "num-switches" = "7"

Received signal 6
#0 0x55cf5aa328ff (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15bda8fe)
#1 0x55cf6c5cbc29 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27773c28)
#2 0x55cf6c2b11c3 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274591c2)
#3 0x55cf6c5ca747 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27772746)
#4 0x7f318edad200 (/usr/lib/x86_64-linux-gnu/libpthread-2.33.so+0x131ff)
#5 0x7f318e2b5891 (/usr/lib/x86_64-linux-gnu/libc-2.33.so+0x3c890)
#6 0x7f318e29f536 (/usr/lib/x86_64-linux-gnu/libc-2.33.so+0x26535)
#7 0x55cf6c5c8cca (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27770cc9)
#8 0x55cf6c3174e1 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274bf4e0)
#9 0x55cf6c318a0e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x274c0a0d)
#10 0x55cf73e53f52 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2effbf51)
#11 0x55cf73e5c718 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2f004717)
#12 0x55cf738101a6 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b81a5)
#13 0x55cf7380d0bf (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b50be)
#14 0x55cf7381093e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2e9b893d)
#15 0x55cf72d613b8 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2df093b7)
#16 0x55cf72d62af2 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2df0aaf1)
#17 0x55cf6c46fa5a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27617a59)
#18 0x55cf6c4e6b5f (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768eb5e)
#19 0x55cf6c4e56be (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768d6bd)
#20 0x55cf6c4e7c42 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2768fc41)

#21 0x55cf6c72dd5d (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x278d5d5c)
#22 0x55cf6c4e8a6b (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27690a6a)
#23 0x55cf6c3e3ccb (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2758bcca)
```

```
#23 0x55cf6c3e3ccb (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2758bcca)
#24 0x55cf60990e54 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb38e53)
#25 0x55cf6099623a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb3e239)
#26 0x55cf6098a44b (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x1bb3244a)
#27 0x55cf6c16243a (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730a439)
#28 0x55cf6c165902 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730d901)
#29 0x55cf6c164bc1 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x2730cbc0)
#30 0x55cf6c15e6d8 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x273066d7)
#31 0x55cf6c15ed6e (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x27306d6d)
#32 0x55cf5aaac136 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15c54135)
#33 0x55cf5aaabf20 (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15c53f1f)
#34 0x7f318e2a07ed (/usr/lib/x86_64-linux-gnu/libc-2.33.so+0x277ec)
#35 0x55cf5a9f91ea (/usr/local/google/home/zxdan/chromium/src/out/asan/chrome+0x15ba11e9)
  r8: 0000000000000000  r9: 00007ffec558f0c0 r10: 0000000000000008 r11: 0000000000000246
 r12: 00007f318c56c000 r13: 00000fe6318ada4c r14: 00000fe6b18a5800 r15: 00007f318c56d250
  di: 0000000000000002  si: 00007ffec558f0c0  bp: 00007ffec558f310  bx: 00007f318de7fa80
  dx: 0000000000000000  ax: 0000000000000000  cx: 00007f318e2b5891  sp: 00007ffec558f0c0
  ip: 00007f318e2b5891 efl: 0000000000000246 cgf: 002b000000000033 erf: 0000000000000000
 trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]
```

Comment 33 by rheza...@gmail.com on Mon, Feb 14, 2022, 2:00 PM EST

zxdan@,

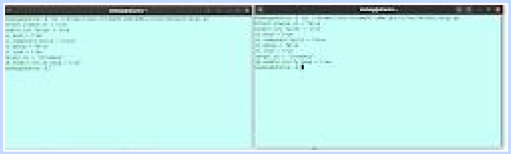
I really sorry for this trouble and didn't meant to make it hard to repro. Based stack trace on #32, it caused when do split view and dcheck_always_on = on. It is same mine stack trace on #28.

If you want to try another one:
(1) please build ASAN locally with `dcheck_always_on = false`
(2) Download pre-built linux-chromeOS from https://www.googleapis.com/download/storage/v1/b/chromium-browser-asan/o/linux-release-chromeos%2Fasan-linux-release-970683.zip?generation=1644863075447382&alt=media

---- This question for security sheriff or allenwebb@google.com ----

I have questions:
(1) Why I'm getting different stack trace if I build Asan locally with args:
 (1a) `dcheck_always_on = on`. got same stack trace on #c32.
 (1b) `dcheck_always_on = false`. got UaF similar my stack on #c0.

Screenshot from 2022-02-15 01-59-26.png
102 KB View Download



Comment 34 by zxdan@chromium.org on Mon, Feb 14, 2022, 2:03 PM EST Project Member

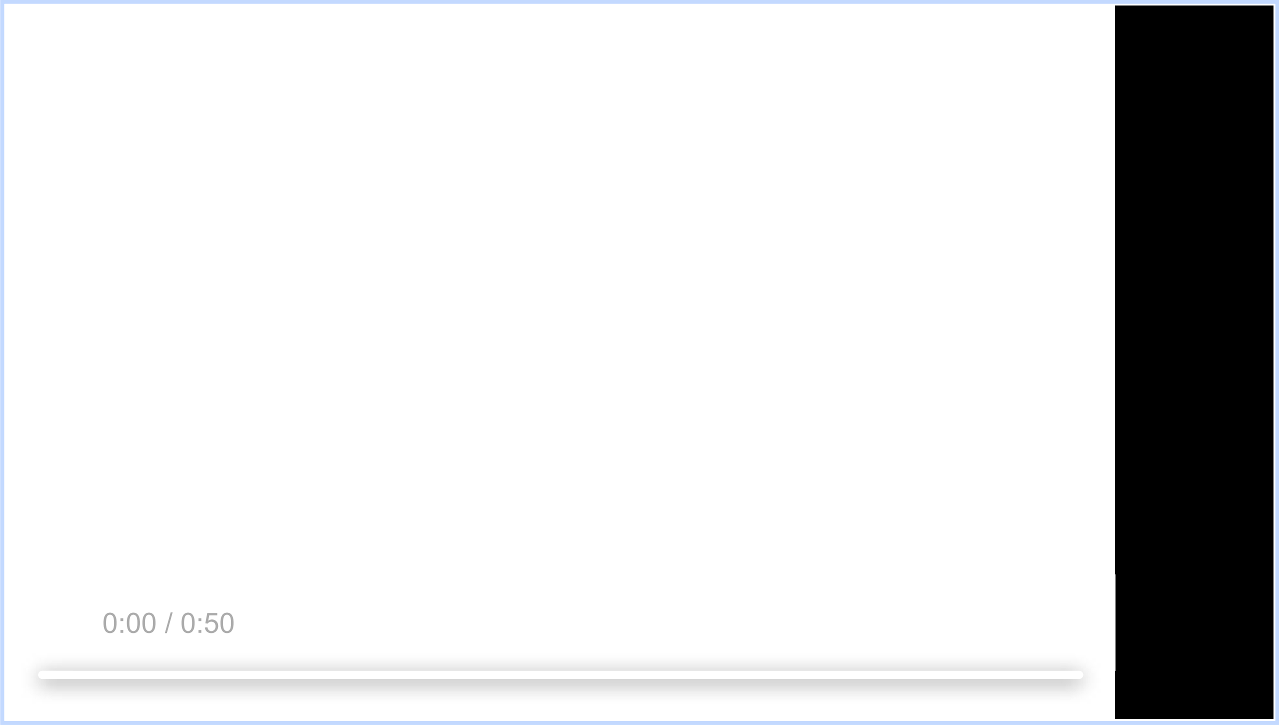
rhezashan@, no worries at all! Thanks so much for reporting this issue. Let's figure it out.

Comment 35 by rheza...@gmail.com on Mon, Feb 14, 2022, 2:08 PM EST
Uploading new screencast on Latest version Chromium 100.0.4890.0 @970683.

I'm sure if you build with `dcheck_always_on = false`, you won't get crash Check failed: window &&

I'm sure if you build with `dcheck_always_on = false` you won't get crash Check failed: window && CanSnapWindow(window).

screencast__00007.webm
7.2 MB View Download



Comment 36 by rheza...@gmail.com on Mon, Feb 14, 2022, 2:17 PM EST

Re #34:
I missed your comment.

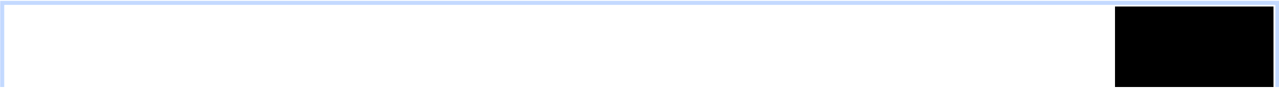
Did you try to test on pre-built ASAN [1]?

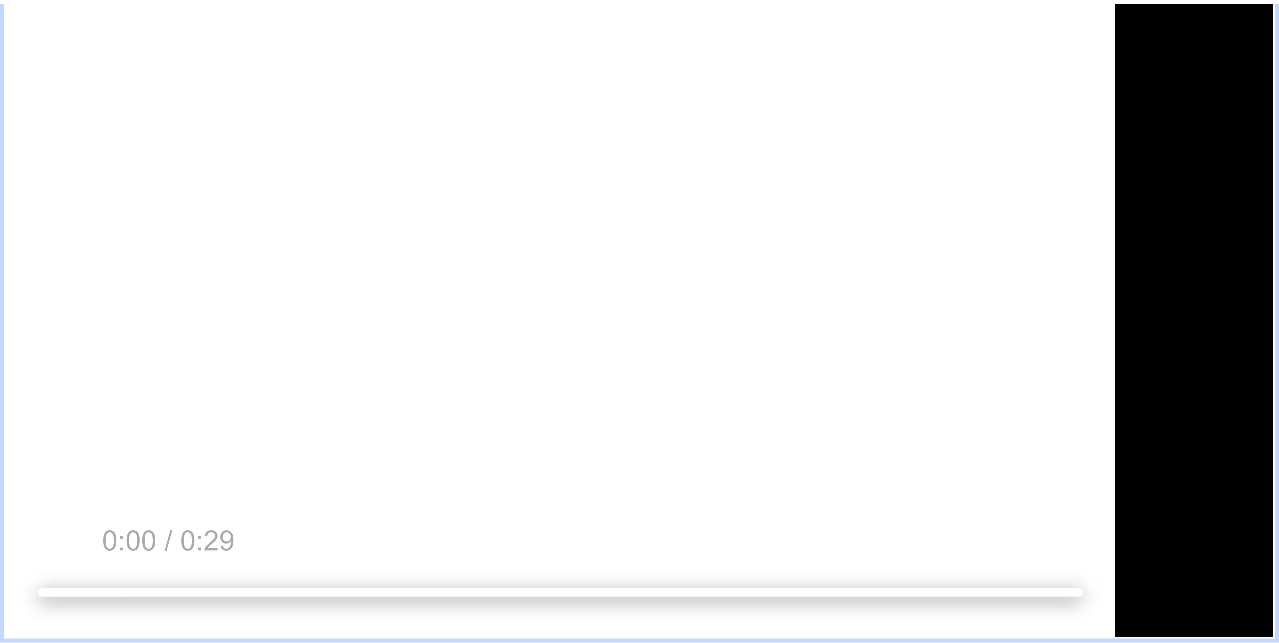
[1] https://commondatastorage.googleapis.com/chromium-browser-asan/index.html?prefix=linux-release-chromeos/asan-linux-release-97

Comment 37 by zxdan@chromium.org on Tue, Feb 22, 2022, 3:21 PM EST Project Member

Fixed the issue with a simple modification. Just prevent the window from being snapped when the window is being destroyed.

Screen recording 2022-02-22 12.00.20 PM.webm
2.9 MB View Download





Comment 38 by allenwebb@google.com on Tue, Feb 22, 2022, 3:25 PM EST Project Member

Are there similar cases that should be covered in the same way (e.g. anything that might animate the window)?

Comment 39 by zxdan@chromium.org on Tue, Feb 22, 2022, 4:31 PM EST Project Member

allenwebb@, could you provide more details about the question in comment 38? Thanks!

Comment 40 by allenwebb@google.com on Tue, Feb 22, 2022, 4:41 PM EST Project Member

There are a few other use-after-free's that were reported about the same time and might have similar causes. I can CC you on them.

Comment 41 by zxdan@chromium.org on Tue, Feb 22, 2022, 4:42 PM EST Project Member

Thanks so much! Please cc them to me.

Comment 42 by allenwebb@google.com on Tue, Feb 22, 2022, 4:45 PM EST Project Member

It looks like the are different causes after re-reading the most recent comments on those threads. I did CC you on a new bug that might be related.

Comment 43 by rheza...@gmail.com on Tue, Feb 22, 2022, 4:57 PM EST

zxdan@

thanks for fixing the issue, as soon as the fix is landed I will test on my side.

Comment 44 by zxdan@chromium.org on Tue, Feb 22, 2022, 5:04 PM EST Project Member

Yes, I saw the new bug. I think it might be caused by a different reason. However, I failed to reproduce the issue on ToT.

Comment 45 by zxdan@chromium.org on Tue, Feb 22, 2022, 5:04 PM EST Project Member

rhezashan@, thanks so much!

Comment 46 by Git Watcher on Wed, Feb 23, 2022, 2:26 PM EST Project Member

The following revision refers to this bug:

https://chromium.googlesource.com/chromium/src/+/b35a7847d73d0e0631229506095b817db25cf40a

commit b35a7847d73d0e0631229506095b817db25cf40a
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Wed Feb 23 19:25:05 2022

Fix the crash of dragging a window in split view

This CL fixes the issues that when dragging a window in split view
while the window is being destroyed, there will be a crash caused
by the DCHECK in SplitViewController::SnapWindow.

We should set is_being_destroyed argument as true in function
SplitViewController::EndWindowDragImpl when the window is being
destroyed to prevent it from being snapped.

~~Bug: 1291986~~
Change-Id: Id9a9339fdc0fd38d07fde3924f25d782d5db256c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482023
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Commit-Position: refs/heads/main@{#974271}

[modify] https://crrev.com/b35a7847d73d0e0631229506095b817db25cf40a/ash/wm/splitview/split_view_controller.cc

Comment 47 by rheza...@gmail.com on Wed, Feb 23, 2022, 4:51 PM EST

zxdan@,

I've tested ~20 times, on version >974271 and the crash didn't happen anymore. The fix in #c46 seems to work.

Comment 48 by zxdan@chromium.org on Wed, Feb 23, 2022, 6:19 PM EST Project Member

rhezashan@, thanks so much for confirming this!! I will add a regression test as well.

Comment 49 by Git Watcher on Fri, Feb 25, 2022, 12:02 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/137f63c76b518c5e4bb81bfbd3b285cd4431527f

commit 137f63c76b518c5e4bb81bfbd3b285cd4431527f
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Fri Feb 25 05:01:08 2022

cros test: destroy a dragged window in split view

This CL adds a regression test that destroying a window which is
dragged from shelf will not cause crash.

Validated that before the fix in crrev.com/c/3482023, the test has
the same crash in crbug/1291986. After fix, there is no crash.

~~Bug: 1291986~~
Change-Id: Id06eaf2c92b41abb4f0829fa44b389bddd066361
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3488101

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3488101
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Commit-Position: refs/heads/main@{#975007}

[modify] https://crrev.com/137f63c76b518c5e4bb81bfbd3b285cd4431527f/ash/shelf/drag_window_from_shelf_controller_unittest.cc

Comment 50 by zxdan@chromium.org on Fri, Feb 25, 2022, 12:09 AM EST Project Member

Status: Fixed (was: Started)

Comment 51 by sheriffbot on Sun, Feb 27, 2022, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 52 by sheriffbot on Sun, Feb 27, 2022, 1:40 PM EST Project Member

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

Comment 53 by sheriffbot on Sun, Feb 27, 2022, 2:00 PM EST Project Member

Labels: Merge-Request-100 Merge-Request-98 Merge-Request-99

Requesting merge to stable M98 because latest trunk commit (975007) appears to be after stable branch point (950365).

Requesting merge to beta M99 because latest trunk commit (975007) appears to be after beta branch point (961656).

Requesting merge to dev M100 because latest trunk commit (975007) appears to be after dev branch point (972766).

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

Comment 54 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

Labels: -Merge-Request-100 Merge-Approved-100 Hotlist-Merge-Approved

Merge approved: your change passed merge requirements and is auto-approved for M100. Please go ahead and merge the CL to branch 4896 (refs/branch-heads/4896) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 55 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

Labels: -Merge-Request-99 Hotlist-Merge-Review Merge-Review-99

Merge review required: M99 has already been cut for stable release.

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?

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), ceb (ChromeOS), pbommana (Desktop)

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

Comment 56 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

Labels: -Merge-Request-98 Merge-Review-98

Merge review required: M98 is already shipping to stable.

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: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 57 by zxdan@chromium.org on Mon, Feb 28, 2022, 1:57 PM EST Project Member

1. Why does your merge fit within the merge criteria for these milestones?
The CLs are solve this heap-use-after-free issue.

2. What changes specifically would you like to merge? Please link to Gerrit.
crrev.com/c/3482023
crrev.com/c/3488101

3. Have the changes been released and tested on canary?
Yes.

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
No. This is not a new feature.

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
Yes.

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.
Yes, it addresses a major issue. A regression test is added but it will be great if a manual test is performed.
- Enter Tablet mode

- Enter Tablet mode.
- Open a window and drag it from shelf to the split view.
- Open a browser window and drag it from shelf to another side of split view.
- setup page close on http.server or with https://www.w3schools.com/jsref/tryit.asp?filename=tryjsref_win_close and modify the original code become
```
<!DOCTYPE html>
<html>
<body>

<h1>The Window Object</h1>
<h2>The open() and close() Methods</h2>

<button onclick="openWin()">Open "myWindow"</button>
<button onclick="closeWin()">Close "myWindow"</button>

<script>
let myWindow;

function openWin() {
  myWindow = window.open(".", ".", "width=200,height=100");
  setTimeout(function(){closeWin();},4000);
}

function closeWin() {
  myWindow.close();
}
</script>

</body>
</html>
````
- click run and click button "open 'myWindow'"
- Drag the opened window from shelf and hold it until the window is closed automatically.
- Check if there is a crash.

Comment 58 by Git Watcher on Mon, Feb 28, 2022, 4:09 PM EST Project Member

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/81faaaf4f0efc219164933a5cce0c9a1820f25b

commit 81faaaf4f0efc219164933a5cce0c9a1820f25b
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Mon Feb 28 21:08:15 2022

[Merge M100] Fix the crash of dragging a window in split view

This CL fixes the issues that when dragging a window in split view
while the window is being destroyed, there will be a crash caused
by the DCHECK in SplitViewController::SnapWindow.

We should set is_being_destroyed argument as true in function
SplitViewController::EndWindowDragImpl when the window is being

SplitViewController::EndWindowDragImpl when the window is being
destroyed to prevent it from being snapped.

(cherry picked from commit b35a7847d73d0e0631229506095b817db25cf40a)

~~Bug: 1291986~~
Change-Id: Id9a9339fdc0fd38d07fde3924f25d782d5db256c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482023
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#974271}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3495823
Cr-Commit-Position: refs/branch-heads/4896@{#151}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify] https://crrev.com/81faaaaf4f0efc219164933a5cce0c9a1820f25b/ash/wm/splitview/split_view_controller.cc

Comment 59 by sheriffbot on Mon, Feb 28, 2022, 4:13 PM EST Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 60 by zxdan@chromium.org on Mon, Feb 28, 2022, 4:18 PM EST Project Member

The issue is because we didn't consider the case when a window is closed while dragging from shelf in split view. I think it is not related to a certain milestone or a change.

Comment 61 by Git Watcher on Mon, Feb 28, 2022, 4:23 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f66d0f81d2f08b751b9784ca403172a2f9ab34c3

commit f66d0f81d2f08b751b9784ca403172a2f9ab34c3
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Mon Feb 28 21:22:24 2022

[Merge M100] cros test: destroy a dragged window in split view

This CL adds a regression test that destroying a window which is
dragged from shelf will not cause crash.

Validated that before the fix in crrev.com/c/3482023, the test has
the same crash in crbug/1291986. After fix, there is no crash.

(cherry picked from commit 137f63c76b518c5e4bb81bfbd3b285cd4431527f)

~~Bug: 1291986~~
Change-Id: Id06eaf2c92b41abb4f0829fa44b389bddd066361
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3488101
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#975007}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3495844
Cr-Commit-Position: refs/branch-heads/4896@{#154}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify] https://crrev.com/f66d0f81d2f08b751b9784ca403172a2f9ab34c3/ash/shelf/drag_window_from_shelf_controller_unittest.cc

Comment 62 by rzanoni@google.com on Tue, Mar 1, 2022, 3:36 AM EST Project Member

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 63 by rzanoni@google.com on Tue, Mar 1, 2022, 4:54 AM EST Project Member

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

Comment 64 by sheriffbot on Tue, Mar 1, 2022, 5:00 AM EST 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 65 by rzanoni@google.com on Tue, Mar 1, 2022, 5:05 AM EST Project Member

1. Just https://crrev.com/c/3497035
2. Low, no conflicts
3. 100
4. Yes

Comment 66 by ceb@google.com on Tue, Mar 1, 2022, 11:06 AM EST Project Member

Labels: -Merge-Review-99 Merge-Approved-99

Merge approved for M99.

Comment 67 by gmpritchard@google.com on Tue, Mar 1, 2022, 1:09 PM EST Project Member

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

I will delay the approval for LTS-96 until the next respin, since it just got M100 and M99 and not tested there yet.

Comment 68 by zxdan@chromium.org on Tue, Mar 1, 2022, 1:13 PM EST Project Member

rzanoni@, I also have a CL about regession test: crrev.com/c/3488101. Shall I also merge it back?

Comment 69 by amyressler@google.com on Thu, Mar 3, 2022, 5:23 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-7000

*** 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 70 by amyressler@chromium.org on Thu, Mar 3, 2022, 5:31 PM EST Project Member

Congratulations! The VRP Panel has decided to award you $7,000 for this report. Thank you for your efforts and reporting this issue to us!

Comment 71 by sheriffbot on Fri, Mar 4, 2022, 12:19 PM EST Project Member

Cc: ceb@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 72 by Git Watcher on Fri, Mar 4, 2022, 3:12 PM EST Project Member

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/106b06e760b2c41af6d89a3f7e9634db72776f6c

commit 106b06e760b2c41af6d89a3f7e9634db72776f6c
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Fri Mar 04 20:11:24 2022

[Merge to M99] Fix the crash of dragging a window in split view

This CL fixes the issues that when dragging a window in split view
while the window is being destroyed, there will be a crash caused
by the DCHECK in SplitViewController::SnapWindow.

We should set is_being_destroyed argument as true in function
SplitViewController::EndWindowDragImpl when the window is being

SplitViewController::EndWindowDragImpl when the window is being
destroyed to prevent it from being snapped.

(cherry picked from commit b35a7847d73d0e0631229506095b817db25cf40a)

~~Bug: 1291986~~
Change-Id: Id9a9339fdc0fd38d07fde3924f25d782d5db256c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482023
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#974271}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499624
Cr-Commit-Position: refs/branch-heads/4844@{#971}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify] https://crrev.com/106b06e760b2c41af6d89a3f7e9634db72776f6c/ash/wm/splitview/split_view_controller.cc

Comment 73 by Git Watcher on Fri, Mar 4, 2022, 3:42 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/dea3b599a82630f9535698d97187907462090676

commit dea3b599a82630f9535698d97187907462090676
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Fri Mar 04 20:41:45 2022

[Merge to M99] cros test: destroy a dragged window in split view

This CL adds a regression test that destroying a window which is
dragged from shelf will not cause crash.

Validated that before the fix in crrev.com/c/3482023, the test has
the same crash in crbug/1291986. After fix, there is no crash.

(cherry picked from commit 137f63c76b518c5e4bb81bfbd3b285cd4431527f)

~~Bug: 1291986~~
Change-Id: Id06eaf2c92b41abb4f0829fa44b389bddd066361
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3488101
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#975007}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3502750
Cr-Commit-Position: refs/branch-heads/4844@{#972}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]
https://crrev.com/dea3b599a82630f9535698d97187907462090676/ash/shelf/drag_window_from_shelf_controller_unittest.cc

Comment 74 by amyressler@google.com on Fri, Mar 11, 2022, 2:59 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 75 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:27 PM EST Project Member

Labels: Release-1-M99

Comment 76 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0974 CVE_description-missing

Comment 77 by gmpritchard@google.com on Tue, Mar 15, 2022, 9:57 AM EDT Project Member

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 78 by Git Watcher on Thu, Mar 17, 2022, 7:31 AM EDT Project Member

Labels: merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ee261b6eb59a6d1498233e7c418678a204ea05dd

commit ee261b6eb59a6d1498233e7c418678a204ea05dd
Author: Xiaodan Zhu <zxdan@chromium.org>
Date: Thu Mar 17 11:30:41 2022

[M96-LTS] Fix the crash of dragging a window in split view

This CL fixes the issues that when dragging a window in split view
while the window is being destroyed, there will be a crash caused
by the DCHECK in SplitViewController::SnapWindow.

We should set is_being_destroyed argument as true in function
SplitViewController::EndWindowDragImpl when the window is being
destroyed to prevent it from being snapped.

(cherry picked from commit b35a7847d73d0e0631229506095b817db25cf40a)

~~Bug: 1291986~~
Change-Id: Id9a9339fdc0fd38d07fde3924f25d782d5db256c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482023
Commit-Queue: Xiaodan Zhu <zxdan@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#974271}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3497035
Reviewed-by: Xiaoqian Dai <xdai@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1537}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/ee261b6eb59a6d1498233e7c418678a204ea05dd/ash/wm/splitview/split_view_controller.cc

Comment 79 by rzanoni@google.com on Thu, Mar 17, 2022, 8:52 AM EDT Project Member

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

Comment 80 by sheriffbot on Fri, Jun 3, 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 81 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 82 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:14 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing