Starred by 3 users

Owner:	sky@chromium.org
CC:	cthomp@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Aura
Modified:	Aug 19, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-90
Target-89
Target-90
merge-merged-4240
LTS-Security-86
external_security_report
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
merge-merged-4430_101
Release-3-M90
CVE-2021-30510

Issue 1197436: Security: heap-use-after-free in DesktopWindowTreeHostPlatform::SetFullscreen

Reported by merc...@gmail.com on Fri, Apr 9, 2021, 4:06 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.114 Safari/537.36

Steps to reproduce the problem:
1. download asan-linux-release-870856.zip and poc.html, unzip chrome.
2. start a server at floder of poc.html : python -m SimpleHTTPServer 8605
3. ./asan-linux-release-870856/chrome http://127.0.0.1:8605/poc.html about:blank
4. click the button, then drag and drop the first tab repeatedly

What is the expected behavior?

What went wrong?
This problem is similar to ~~issues 1170635~~.

When Drop and drop a tab to another tab to merge them, the origin tab will be closed and recreated. So if we call FullScreen(with the help of timeout) when the origin tab is closed, the freed `BrowserDesktopWindowTreeHostLinux` will be used, UAF occurs.
The FullScreen should be called right after the tab is closed, so you need to drag and drop multitimes to reproduce this.

PS:
Note that there is also a CHECK fail in this poc, but it is a different crash to this UAF.(It seems that CHECK fail is not security bug). After click the button, you can drag the tab and don't release the mouse, when this tab become fullscreen, move mouse to the origin position of the tab, CHECK failed occured, as shown in video.

```
=================================================================
==17411==ERROR: AddressSanitizer: heap-use-after-free on address 0x61700054d988 at pc 0x56426d903111 bp 0x7ffcba366ef0 sp 0x7ffcba366ee8
READ of size 8 at 0x61700054d988 thread T0 (chrome)
    #0 0x56426d903110 in SetFullscreen ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc:630:7
    #1 0x56426d903110 in non-virtual thunk to views::DesktopWindowTreeHostPlatform::SetFullscreen(bool)
ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
    #2 0x56426d7ed52e in views::Widget::SetFullscreen(bool) ui/views/widget/widget.cc:759:19
    #3 0x56426e96d398 in BrowserView::ProcessFullscreen(bool, GURL const&, ExclusiveAccessBubbleType, long) chrome/browser/ui/views/frame/browser_view.cc:3346:11
    #4 0x56426e96d9df in EnterFullscreen chrome/browser/ui/views/frame/browser_view.cc:1357:3
    #5 0x56426e96d9df in non-virtual thunk to BrowserView::EnterFullscreen(GURL const&, ExclusiveAccessBubbleType, long)
chrome/browser/ui/views/frame/browser_view.cc
    #6 0x56426e2acf7c in FullscreenController::EnterFullscreenModeInternal(FullscreenController::FullscreenInternalOption, content::RenderFrameHost*, long)
chrome/browser/ui/exclusive_access/fullscreen_controller.cc:407:42
    #7 0x56426e2ac521 in FullscreenController::EnterFullscreenModeForTab(content::RenderFrameHost*, long)
chrome/browser/ui/exclusive_access/fullscreen_controller.cc:164:5
    #8 0x56425be8c35e in content::WebContentsImpl::EnterFullscreenMode(content::RenderFrameHostImpl*, blink::mojom::FullscreenOptions const&)
content/browser/web_contents/web_contents_impl.cc:3149:16
    #9 0x56425b99565b in content::RenderFrameHostImpl::EnterFullscreen(mojo::InlinedStructPtr<blink::mojom::FullscreenOptions>, base::OnceCallback<void (bool)>)
content/browser/renderer_host/render_frame_host_impl.cc:4886:14
    #10 0x564258b2809c in blink::mojom::LocalFrameHostStubDispatch::AcceptWithResponder(blink::mojom::LocalFrameHost*, mojo::Message*,
std::__1::unique_ptr<mojo::MessageReceiverWithStatus, std::__1::default_delete<mojo::MessageReceiverWithStatus> >)
gen/third_party/blink/public/mojom/frame/frame.mojom.cc:6602:13
    #11 0x564264c942b6 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*) mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:526:56
```

```
    #12 0x564264c9ff8a in mojo::MessageDispatcher::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/message_dispatcher.cc:48:24
    #13 0x56426657e9c9 in IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptOnProxyThread(mojo::Message) ipc/ipc_mojo_bootstrap.cc:945:24
    #14 0x5642665772e4 in Invoke<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message), scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController>, mojo::Message> base/bind_internal.h:509:12
    #15 0x5642665772e4 in MakeItSo<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message), scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController>, mojo::Message> base/bind_internal.h:648:12
    #16 0x5642665772e4 in RunImpl<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message), std::tuple<scoped_refptr<IPC::
(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>, 0, 1> base/bind_internal.h:721:12
    #17 0x5642665772e4 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:690:12
    #18 0x5642633829a6 in Run base/callback.h:101:12
    #19 0x5642633829a6 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:173:33
    #20 0x5642633bc4d0 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #21 0x5642633bbcd4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #22 0x564263280999 in HandleDispatch base/message_loop/message_pump_glib.cc:374:46
    #23 0x564263280999 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) base/message_loop/message_pump_glib.cc:124:43
    #24 0x7ffaacf2dfbc in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51fbc)

0x61700054d988 is located 8 bytes inside of 688-byte region [0x61700054d980,0x61700054dc30)
freed by thread T0 (chrome) here:
    #0 0x564255f0a85d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x56426d8c5104 in operator() buildtools/third_party/libc++/trunk/include/memory:1335:5
    #2 0x56426d8c5104 in reset buildtools/third_party/libc++/trunk/include/memory:1596:7
    #3 0x56426d8c5104 in views::DesktopNativeWidgetAura::OnHostClosed() ui/views/widget/desktop_aura/desktop_native_widget_aura.cc:335:9
    #4 0x56426d8b1bab in views::DesktopWindowTreeHostLinux::OnClosed() ui/views/widget/desktop_aura/desktop_window_tree_host_linux.cc:251:34
    #5 0x56426d8fc4e3 in views::DesktopWindowTreeHostPlatform::CloseNow() ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc:314:22
    #6 0x56426d906094 in Invoke<void (views::DesktopWindowTreeHostPlatform::*)(), base::WeakPtr<views::DesktopWindowTreeHostPlatform>>
base/bind_internal.h:509:12
    #7 0x56426d906094 in MakeItSo<void (views::DesktopWindowTreeHostPlatform::*)(), base::WeakPtr<views::DesktopWindowTreeHostPlatform>>
base/bind_internal.h:668:5
    #8 0x56426d906094 in RunImpl<void (views::DesktopWindowTreeHostPlatform::*)(), std::tuple<base::WeakPtr<views::DesktopWindowTreeHostPlatform> >, 0>
base/bind_internal.h:721:12
    #9 0x56426d906094 in base::internal::Invoker<base::internal::BindState<void (views::DesktopWindowTreeHostPlatform::*)(),
base::WeakPtr<views::DesktopWindowTreeHostPlatform> >, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #10 0x5642633829a6 in Run base/callback.h:101:12
    #11 0x5642633829a6 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:173:33
    #12 0x5642633bc4d0 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #13 0x5642633bbcd4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #14 0x56426327fc20 in base::MessagePumpGlib::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_glib.cc:404:48
    #15 0x5642633bd767 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:457:12
    #16 0x564263302831 in base::RunLoop::Run(base::Location const&) base/run_loop.cc:133:14
    #17 0x56426777794b in ui::X11WholeScreenMoveLoop::RunMoveLoop(bool, scoped_refptr<ui::X11Cursor>, scoped_refptr<ui::X11Cursor>)
ui/base/x/x11_whole_screen_move_loop.cc:196:12
    #18 0x56426d902237 in views::DesktopWindowTreeHostPlatform::RunMoveLoop(gfx::Vector2d const&, views::Widget::MoveLoopSource,
views::Widget::MoveLoopEscapeBehavior) ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc:571:47
    #19 0x56426efefa60 in TabDragController::RunMoveLoop(gfx::Vector2d const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:1423:61
    #20 0x56426eff48ba in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:1390:3
    #21 0x56426eff23f1 in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:865:5
    #22 0x56426eff0385 in TabDragController::ContinueDragging(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:831:9
    #23 0x56426efe9792 in TabDragController::Drag(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:604:7
    #24 0x56426eff1275 in TabDragController::OnWidgetBoundsChanged(views::Widget*, gfx::Rect const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:688:3
    #25 0x56426d7f60a6 in views::Widget::OnNativeWidgetSizeChanged(gfx::Size const&) ui/views/widget/widget.cc:1234:14
    #26 0x56426d8cd47d in OnHostResized ui/views/widget/desktop_aura/desktop_native_widget_aura.cc:1274:28
    #27 0x56426d8cd47d in non-virtual thunk to views::DesktopNativeWidgetAura::OnHostResized(aura::WindowTreeHost*)
ui/views/widget/desktop_aura/desktop_native_widget_aura.cc
    #28 0x564268c52740 in aura::WindowTreeHost::OnHostResizedInPixels(gfx::Size const&) ui/aura/window_tree_host.cc:468:14
    #29 0x56426d8b5e71 in aura::WindowTreeHostPlatform::OnBoundsChanged(ui::PlatformWindowDelegate::BoundsChange const&)
ui/aura/window_tree_host_platform.cc:228:5
    #30 0x564267754a27 in ui::X11Window::ToggleFullscreen() ui/platform_window/x11/x11_window.cc:637:30
    #31 0x56426d902fd4 in SetFullscreen ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc:624:22
    #32 0x56426d902fd4 in non-virtual thunk to views::DesktopWindowTreeHostPlatform::SetFullscreen(bool)
ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
    #33 0x56426d7ed52e in views::Widget::SetFullscreen(bool) ui/views/widget/widget.cc:759:19
    #34 0x56426e96d398 in BrowserView::ProcessFullscreen(bool, GURL const&, ExclusiveAccessBubbleType, long)
chrome/browser/ui/views/frame/browser_view.cc:3346:11
    #35 0x56426e96d9df in EnterFullscreen chrome/browser/ui/views/frame/browser_view.cc:1357:3
    #36 0x56426e96d9df in non-virtual thunk to BrowserView::EnterFullscreen(GURL const&, ExclusiveAccessBubbleType, long)
chrome/browser/ui/views/frame/browser_view.cc
    #37 0x56426e2acf7c in FullscreenController::EnterFullscreenModeInternal(FullscreenController::FullscreenInternalOption, content::RenderFrameHost*, long)
chrome/browser/ui/exclusive_access/fullscreen_controller.cc:407:42
    #38 0x56426e2ac521 in FullscreenController::EnterFullscreenModeForTab(content::RenderFrameHost*, long)
chrome/browser/ui/exclusive_access/fullscreen_controller.cc:164:5

previously allocated by thread T0 (chrome) here:
    #0 0x564255f09ffd in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x56426eacd349 in BrowserDesktopWindowTreeHost::CreateBrowserDesktopWindowTreeHost(views::internal::NativeWidgetDelegate*,
views::DesktopNativeWidgetAura*, BrowserView*, BrowserFrame*) chrome/browser/ui/views/frame/browser_desktop_window_tree_host_linux.cc:162:10
    #2 0x56426f2c1091 in DesktopBrowserFrameAura::InitNativeWidget(views::Widget::InitParams) chrome/browser/ui/views/frame/desktop_browser_frame_aura.cc:53:7
    #3 0x56426d7e4b81 in views::Widget::Init(views::Widget::InitParams) ui/views/widget/widget.cc:364:19
    #4 0x56426e989c2e in BrowserFrame::InitBrowserFrame() chrome/browser/ui/views/frame/browser_frame.cc:114:3
    #5 0x56426eabffd3 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 0x56426e1f49a5 in CreateBrowserWindow chrome/browser/ui/browser.cc:302:10
    #7 0x56426e1f49a5 in Browser::Browser(Browser::CreateParams const&) chrome/browser/ui/browser.cc:511:29
    #8 0x56426e1f33d6 in Browser::Create(Browser::CreateParams const&) chrome/browser/ui/browser.cc:433:14
    #9 0x56426effa84a in TabDragController::CreateBrowserForDrag(TabDragContext*, gfx::Point const&, gfx::Vector2d*, std::__1::vector<gfx::Rect,
std::__1::allocator<gfx::Rect> >*) chrome/browser/ui/views/tabs/tab_drag_controller.cc:2072:22
    #10 0x56426eff451b in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:1348:22
    #11 0x56426eff23f1 in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:865:5
    #12 0x56426eff0385 in TabDragController::ContinueDragging(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:831:9
    #13 0x56426efe9792 in TabDragController::Drag(gfx::Point const&) chrome/browser/ui/views/tabs/tab_drag_controller.cc:604:7
    #14 0x56426f025450 in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) chrome/browser/ui/views/tabs/tab_strip.cc:456:25
    #15 0x56426f0321e3 in TabStrip::OnMouseDragged(ui::MouseEvent const&) chrome/browser/ui/views/tabs/tab_strip.cc:3745:3
    #16 0x56426d77fa8b in views::View::ProcessMouseDragged(ui::MouseEvent*) ui/views/view.cc:2996:9
    #17 0x5642666e0df0 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #18 0x5642666de719 in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #19 0x5642666de719 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
```

```
    #20 0x5642666ddfe1 in DispatchEventToTarget ui/events/event_dispatcher.cc:84:14
    #21 0x5642666ddfe1 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #22 0x56426d7d7c30 in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) ui/views/widget/root_view.cc:457:9
    #23 0x56426d7f6f50 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc:1347:22
    #24 0x5642666e0df0 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #25 0x5642666de719 in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #26 0x5642666de719 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #27 0x5642666ddfe1 in DispatchEventToTarget ui/events/event_dispatcher.cc:84:14
    #28 0x5642666ddfe1 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #29 0x564268c3917d in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #30 0x564268c56e4f in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:113:16
    #31 0x564268c56af3 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*) ui/events/event_source.cc:138:12
    #32 0x56426d8b6887 in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*) ui/aura/window_tree_host_platform.cc:246:38
    #33 0x56426d8b17b6 in views::DesktopWindowTreeHostLinux::DispatchEvent(ui::Event*) ui/views/widget/desktop_aura/desktop_window_tree_host_linux.cc:245:29
    #34 0x564267761d13 in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event const&) ui/platform_window/x11/x11_window.cc:1191:34

SUMMARY: AddressSanitizer: heap-use-after-free ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc:630:7 in SetFullscreen
Shadow bytes around the buggy address:
  0x0c2e800a1ae0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1af0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b00: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b10: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x0c2e800a1b20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2e800a1b30: fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c2e800a1b80: fd fd fd fd fd fd 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
  Shadow gap:              cc
==17411==ABORTING
```

Did this work before? N/A

Chrome version: Channel: stable
OS Version: ubuntu20
Flash Version:

poc.html
292 bytes View Download

movie.mp4
14.5 MB View Download

Comment 1 by sheriffbot on Fri, Apr 9, 2021, 4:09 AM EDT Project Member

Labels: external_security_report

Comment 2 by cthomp@chromium.org on Fri, Apr 9, 2021, 2:15 PM EDT Project Member

Labels: Needs-Feedback

Thanks for the report. I can repro the CHECK failure on linux ASAN r870856 by the following steps:

- Start server `python -m SimpleHTTPServer 8605`
- ./chrome --user-data-dir=/tmp/crbug1197436 http://127.0.0.1:8605/poc.html about:blank
- Click the "trigger" button and then drag the tab out of the current window but don't release
- After fullscreen triggers (with mouse still held down) move cursor back to where the first window's tab strip was

That triggers [FATAL:tab_strip_model.cc(1891)] Check failed: ContainsIndex(index). Failed to find: -1 in: 0 entries. This crashes the entire browser.

I'm having trouble reproducing the ASAN failure though. If I follow the steps in the report, I can't get anything to trigger. If I try to match the actions in the second part of the video (dragging the tab out of the window and then back and forth over the other tabstrip) I just trigger the CHECK failure. Do you have any additional guidance for how to reproduce this?

Comment 3 by merc....@gmail.com on Fri, Apr 9, 2021, 10:39 PM EDT

I'm sorry there are no more additional guidance...I also try many many times to trigger UAF. I just cut the video that uaf occurs.

Comment 4 by sheriffbot on Fri, Apr 9, 2021, 10:42 PM EDT Project Member

Cc: cthomp@chromium.org
Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 5 by cthomp@chromium.org on Mon, Apr 12, 2021, 1:37 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: sky@chromium.org
Labels: Security_Severity-High Security_Impact-Stable Pri-1
Components: Internals>Aura

Got it, thanks. I'll try some more to reproduce this today. Tentatively setting some security labels on the presumption that this is reproducible:

- Sev-High for memory corruption in browser process but mitigated by requiring user interactions to trigger the race between tab destruction/creation and fullscreen trigger, but this could potentially be more controlled by something like an extension with the chrome.tabs API
- Impact-Stable because most of the stack trace appears to be unchanged for a while

+sky@ could you take a look? The CHECK failures seem reasonable: we're in an extraordinary situation with this kind interaction, so crashing seems reasonable. I'm not sure if this is "hiding" the use-after-free that could sometimes get triggered (i.e., they tend to co-occur, but the CHECK happens first), as I'm not familiar with this code. A more expert opinion would be appreciated.

Testing in a debug ASAN build (r857956) to see if there is a timing/race issue that might be easier to trigger in a (slower) debug build, I hit a couple DCHECK failures when trying to reproduce this:

[43773:43773:0412/095100.675399:FATAL:tab_strip_model.cc(140)] Check failed: became_visible.
[44724:44724:0412/100757.376620:FATAL:tab_drag_controller.cc(1299)] Check failed: -1 != index (-1 vs. -1)

Comment 6 by sheriffbot on Tue, Apr 13, 2021, 12:47 PM EDT Project Member

Labels: Target-89 M-89

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

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

Comment 7 by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT Project Member

Labels: -M-89 M-90 Target-90

Comment 8 by sheriffbot on Fri, Apr 23, 2021, 12:21 PM EDT Project Member

sky: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

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

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

Comment 9 by sky@chromium.org on Fri, Apr 23, 2021, 4:50 PM EDT Project Member

Status: Started (was: Assigned)

Comment 10 by Git Watcher on Tue, Apr 27, 2021, 7:30 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5e5027e78c4ebe284a35c68ac11a62ae70d6d114

commit 5e5027e78c4ebe284a35c68ac11a62ae70d6d114
Author: Scott Violet <sky@chromium.org>
Date: Tue Apr 27 23:29:51 2021

views: handle deletion when toggling fullscreen

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

Change-Id: Ibd53604ba29ea4bfa6490f65112410bc74eb81dd
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2848379
Commit-Queue: Scott Violet <sky@chromium.org>
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/heads/master@{#876822}

[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/widget/widget.cc
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/5e5027e78c4ebe284a35c68ac11a62ae70d6d114/ui/views/win/hwnd_message_handler.cc

Comment 11 by Git Watcher on Wed, Apr 28, 2021, 12:49 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/17ff04407b35f543622d36c5af4f0301f5c7f0eb

commit 17ff04407b35f543622d36c5af4f0301f5c7f0eb
Author: Melissa Zhang <melzhang@chromium.org>
Date: Wed Apr 28 04:48:28 2021

Revert "views: handle deletion when toggling fullscreen"

This reverts commit 5e5027e78c4ebe284a35c68ac11a62ae70d6d114.

Reason for revert: Breaks builder https://ci.chromium.org/ui/p/chromium/builders/ci/win-asan/18447/overview

Original change's description:
> views: handle deletion when toggling fullscreen
>
> Toggling fullscreen means the bounds change. There are some
> code paths that may delete the Widget when the bounds changes.
> This patch ensures the right thing happens if the Widget is
> deleted when this happens.
>
> ~~BUG=1197436~~
> TEST=DesktopWidgetTest.DestroyInSetFullscreen
>
> Change-Id: Ibd53604ba29ea4bfa6490f65112410bc74eb81dd
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2848379
> Commit-Queue: Scott Violet <sky@chromium.org>
> Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#876822}

~~Bug: 1197436~~
Change-Id: Id5989e42e059a025b5f000828b8a22db4a4e6f13
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2854260
Auto-Submit: Melissa Zhang <melzhang@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Melissa Zhang <melzhang@chromium.org>
Owners-Override: Melissa Zhang <melzhang@chromium.org>
Cr-Commit-Position: refs/heads/master@{#876911}

[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/widget/widget.cc
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/17ff04407b35f543622d36c5af4f0301f5c7f0eb/ui/views/win/hwnd_message_handler.cc

Comment 12 by Git Watcher on Thu, Apr 29, 2021, 5:07 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/60fe7a686c0620855c28a60721f668a99e409ee4

commit 60fe7a686c0620855c28a60721f668a99e409ee4
Author: Scott Violet <sky@chromium.org>
Date: Thu Apr 29 21:06:53 2021

[reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Commit-Position: refs/heads/master@{#877640}

[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/widget/widget.cc
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/60fe7a686c0620855c28a60721f668a99e409ee4/ui/views/win/hwnd_message_handler.cc

Comment 13 by sky@chromium.org on Fri, Apr 30, 2021, 12:55 PM EDT Project Member

Status: Fixed (was: Started)

Comment 14 by sheriffbot on Fri, Apr 30, 2021, 2:02 PM EDT Project Member

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

Comment 15 by sheriffbot on Fri, Apr 30, 2021, 2:22 PM EDT Project Member

Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (877640) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (877640) appears to be after beta branch point (870763).

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

Comment 16 by sheriffbot on Fri, Apr 30, 2021, 5:10 PM EDT Project Member

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

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?

4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 17 by sheriffbot on Sat, May 1, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 18 by adetaylor@google.com on Mon, May 3, 2021, 11:18 AM EDT Project Member

Labels: -Merge-Request-90 -Merge-Review-91 Merge-Approved-91 Merge-Approved-90

Approving merge to M91, branch 4472, and to M90, branch 4430.

Comment 19 by Git Watcher on Mon, May 3, 2021, 8:13 PM EDT Project Member

Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d1d442ec8d495ca9c284784e71f691304d24fd85

commit d1d442ec8d495ca9c284784e71f691304d24fd85
Author: Scott Violet <sky@chromium.org>
Date: Tue May 04 00:12:52 2021

[M90] [reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

(cherry picked from commit 60fe7a686c0620855c28a60721f668a99e409ee4)

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877640}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2868317
Auto-Submit: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1383}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/widget.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/hwnd_message_handler.cc

Comment 20 by Git Watcher on Mon, May 3, 2021, 8:13 PM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9761d225f419e2d242759617461c92b16668f029

commit 9761d225f419e2d242759617461c92b16668f029
Author: Scott Violet <sky@chromium.org>
Date: Tue May 04 00:12:38 2021

[M91] [reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

(cherry picked from commit 60fe7a686c0620855c28a60721f668a99e409ee4)

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877640}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2868965
Auto-Submit: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#706}

Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/widget/widget.cc
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/9761d225f419e2d242759617461c92b16668f029/ui/views/win/hwnd_message_handler.cc

Comment 21 by Git Watcher on Mon, May 3, 2021, 8:14 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d1d442ec8d495ca9c284784e71f691304d24fd85

commit d1d442ec8d495ca9c284784e71f691304d24fd85
Author: Scott Violet <sky@chromium.org>
Date: Tue May 04 00:12:52 2021

[M90] [reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

(cherry picked from commit 60fe7a686c0620855c28a60721f668a99e409ee4)

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877640}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2868317
Auto-Submit: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1383}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/widget.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/d1d442ec8d495ca9c284784e71f691304d24fd85/ui/views/win/hwnd_message_handler.cc

Comment 22 by amyressler@chromium.org on Fri, May 7, 2021, 5:22 PM EDT Project Member

Labels: Release-3-M90

Comment 23 by vsavu@google.com on Mon, May 10, 2021, 9:21 AM EDT Project Member

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

Comment 24 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT Project Member

Labels: CVE-2021-30510 CVE_description-missing

Comment 25 by Git Watcher on Wed, May 12, 2021, 4:19 AM EDT Project Member

Labels: merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14

commit 5dc05677cfa32a06b4fcca9a0c3090ef02a18d14
Author: Scott Violet <sky@chromium.org>
Date: Wed May 12 08:17:28 2021

[M90] [reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

(cherry picked from commit 60fe7a686c0620855c28a60721f668a99e409ee4)

(cherry picked from commit d1d442ec8d495ca9c284784e71f691304d24fd85)

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#877640}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2868317
Auto-Submit: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1383}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884064
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#16}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93ccccа35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/widget/widget.cc
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/5dc05677cfa32a06b4fcca9a0c3090ef02a18d14/ui/views/win/hwnd_message_handler.cc

Comment 26 by gianluca@google.com on Wed, May 12, 2021, 12:33 PM EDT Project Member

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

Comment 27 by Git Watcher on Wed, May 12, 2021, 2:12 PM EDT Project Member

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e

commit 14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e
Author: Scott Violet <sky@chromium.org>
Date: Wed May 12 18:11:04 2021

[reland] views: handle deletion when toggling fullscreen

This differs from the first in so far as needing to add more early
outs in the windows side if destroyed. This was caught by the asan
bot.

Toggling fullscreen means the bounds change. There are some
code paths that may delete the Widget when the bounds changes.
This patch ensures the right thing happens if the Widget is
deleted when this happens.

~~BUG=1197436~~
TEST=DesktopWidgetTest.DestroyInSetFullscreen

(cherry picked from commit 60fe7a686c0620855c28a60721f668a99e409ee4)

Change-Id: I8ce8f2045878b6f6de530f58e386149189900498
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2857227
Reviewed-by: Thomas Anderson <thomasanderson@chromium.org>
Commit-Queue: Scott Violet <sky@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877640}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883762
Reviewed-by: Scott Violet <sky@chromium.org>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1636}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/widget/desktop_aura/desktop_window_tree_host_platform.cc
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/widget/desktop_aura/desktop_window_tree_host_win.cc
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/widget/widget.cc
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/widget/widget_unittest.cc
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/win/fullscreen_handler.cc
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/win/fullscreen_handler.h
[modify] https://crrev.com/14486b12d7aca2e6e21c3c03bf1a0c1c10002a0e/ui/views/win/hwnd_message_handler.cc

Comment 28 by amyressler@google.com on Wed, May 12, 2021, 7:11 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 29 by amyressler@chromium.org on Wed, May 12, 2021, 7:23 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $10,000 for this report. Great work!

Comment 30 by amyressler@google.com on Mon, May 17, 2021, 2:22 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 31 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Thu, Aug 19, 2021, 1:30 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