☆ Starred by 3 users

Owner:	adithyas@chromium.org
CC:	carlosil@chromium.org mcnee@chromium.org vollick@chromium.org jbroman@chromium.org mas...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WindowDialog Blink>Portals
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	3
Type:	Bug-Security

Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
Hotlist-Merge-Reject
CVE_description-submitted
Target-97
external_security_report
M-98
reward-7000
Target-98
FoundIn-97
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
Merge-Reject-98
Merge-Reject-99
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1125

Issue 1292261: Security: Heap-use-after-free in BrowserList::AddBrowser

Reported by chrom...@gmail.com on Sat, Jan 29, 2022, 12:15 AM EST

Code

Chrome Version: 100.0.4858.0 (Developer Build) (x86_64) canary
Operating System: macOS

REPRODUCTION CASE

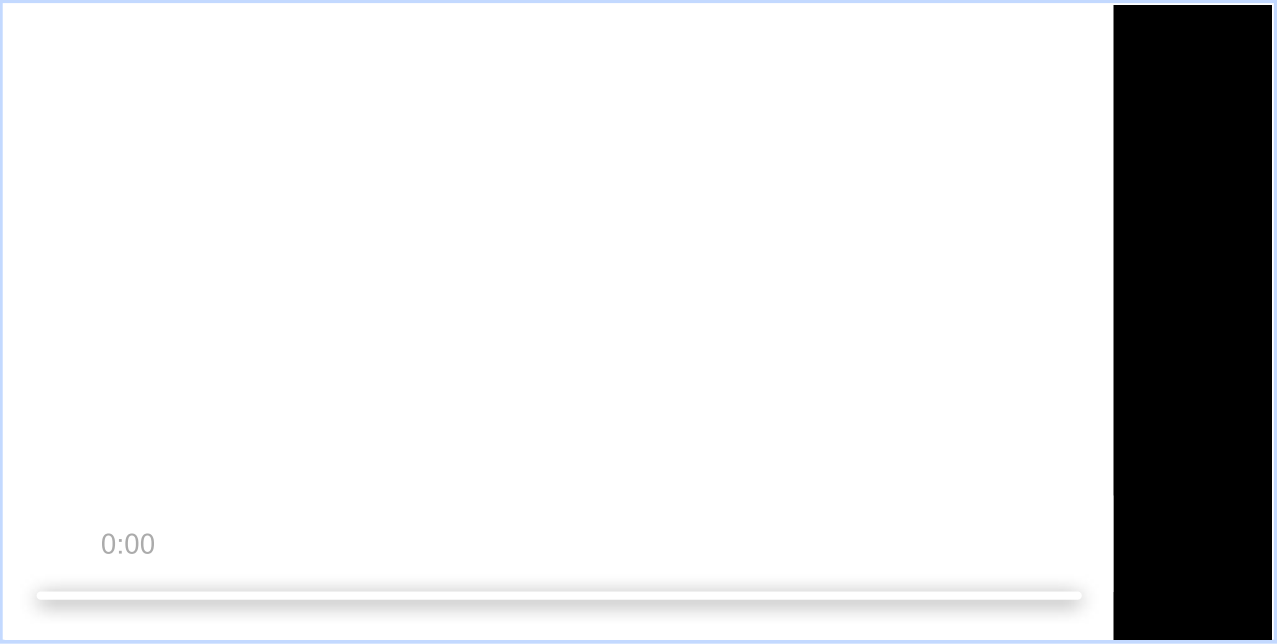
1. Run ./chromium portal.html about:blank
2. drag and drop the portal.html tab repeatedly

(The same method of repro ~~issue 1197436~~).

```
==13126==ERROR: AddressSanitizer: heap-use-after-free on address 0x606000015a48 at pc 0x000127cd213f bp
0x7fff52437d30 sp 0x7fff52437d28
READ of size 8 at 0x606000015a48 thread T0
   #0 0x127cd213e in BrowserList::AddBrowser(Browser*) browser_list.cc:89
   #1 0x127c7158a in Browser::Browser(Browser::CreateParams const&) browser.cc:557
   #2 0x127c6fcfb in Browser::Create(Browser::CreateParams const&) browser.cc:444
   #3 0x128cb4e38 in TabDragController::CreateBrowserForDrag(TabDragContext*, gfx::Point const&, gfx::Vector2d*,
std::__1::vector<gfx::Rect, std::__1::allocator<gfx::Rect> >*) tab_drag_controller.cc:2047
   #4 0x128caffe3 in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&)
tab_drag_controller.cc:1308
   #5 0x128cadbeb in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&)
tab_drag_controller.cc:867
   #6 0x128cac600 in TabDragController::ContinueDragging(gfx::Point const&) tab_drag_controller.cc:837
   #7 0x128ca520f in TabDragController::Drag(gfx::Point const&) tab_drag_controller.cc:601
   #8 0x128d2b55d in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) tab_strip.cc:395
   #9 0x128d3689b in TabStrip::OnMouseDragged(ui::MouseEvent const&) tab_strip.cc:3259
   #10 0x12709856d in views::View::ProcessMouseDragged(ui::MouseEvent*) view.cc:3051
   #11 0x11fff5be2 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:190
   #12 0x11fff5492 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:83
   #13 0x1270d0174 in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) root_view.cc:463
   #14 0x1270ef0aa in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1555
   #15 0x12718ed6c in non-virtual thunk to
views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event>
>) native_widget_mac_ns_window_host.mm:895
   #16 0x1235302db in -[BridgedContentView mouseEvent:] bridged_content_view.mm:618
   #17 0x12352d4ed in -[BridgedContentView processCapturedMouseEvent:] bridged_content_view.mm:300
   #18 0x123560d4b in ___ZN12remote_cocoa17CocoaMouseCapture14ActiveEventTap4InitEv_block_invoke
mouse_capture.mm:92
   #19 0x7fff9d74e7f9 in _NSSendEventToObservers+0x173 (AppKit:x86_64+0x1c77f9) (BuildId:
e39cd61301043e26b424be83ced656f92400000010000000000c0a00000c0a00)
   #20 0x7fff9dd4723e in -[NSApplication(NSEvent) sendEvent:]+0x36 (AppKit:x86_64+0x7c023e) (BuildId:
e39cd61301043e26b424be83ced656f92400000010000000000c0a00000c0a00)
   #21 0x11caea0ac in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:344

   #22 0x11dd817f9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xda077f9)
(BuildId: 4c4c448655553144a17fee2bd4ae26b42400000010000000000b0a0000010c00)
   #23 0x11cae90ba in -[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:331
   #23 0x11cae90ba in -[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:321
   #24 0x7fff9d5c23d6 in -[NSApplication run]+0x3e9 (AppKit:x86_64+0x3b3d6) (BuildId:
e39cd61301043e26b424be83ced656f92400000010000000000c0a00000c0a00)
   #25 0x11dd95cca in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*)
message_pump_mac.mm:743
   #26 0x11dd91a08 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*)
message_pump_mac.mm:161
   #27 0x11dcb0916 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) thread_controller_with_message_pump_impl.cc:468
   #28 0x11dbe39fc in base::RunLoop::Run(base::Location const&) run_loop.cc:140
   #29 0x114cc0512 in content::BrowserMainLoop::RunMainMessageLoop() browser_main_loop.cc:1053
   #30 0x114cc4b51 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:155
   #31 0x114cb9ec5 in content::BrowserMain(content::MainFunctionParams) browser_main.cc:30
   #32 0x11c93b60a in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*)
content_main_runner_impl.cc:641
   #33 0x11c93e3e3 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
content_main_runner_impl.cc:1165
   #34 0x11c93d667 in content::ContentMainRunnerImpl::Run() content_main_runner_impl.cc:1031
   #35 0x11c939fab in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content_main.cc:399
   #36 0x11c93a71d in content::ContentMain(content::ContentMainParams) content_main.cc:427
   #37 0x11037ea91 in ChromeMain chrome_main.cc:176
   #38 0x10d7c4bb5 in main chrome_exe_main_mac.cc:117
   #39 0x7fffb5722234 in start+0x0 (libdyld.dylib:x86_64+0x5234) (BuildId:
4a0e66c1459638e6898ebd2660478d3d2400000010000000000c0a00000c0a00)

0x606000015a48 is located 8 bytes inside of 64-byte region [0x606000015a40,0x606000015a80)
freed by thread T0 here:
   #0 0x10d913019  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x47019) (BuildId:
b4732162098e3d0f8e0b461cd4a220432400000010000000000070a0000010b00)
   #1 0x127a94d2b in javascript_dialogs::TabModalDialogManager::~TabModalDialogManager() unique_ptr.h:54
   #2 0x127a95464 in non-virtual thunk to javascript_dialogs::TabModalDialogManager::~TabModalDialogManager()
tab_modal_dialog_manager.cc:116
   #3 0x11dc5e055 in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) unique_ptr.h:54
   #4 0x11dc5dfed in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
   #5 0x11dc5dfed in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,

std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
   #6 0x11dc5e00c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
   #7 0x11dc5e00c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
   #8 0x11dc5e00c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
   #9 0x11dc5dfed in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1798
   #10 0x11dc5e00c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*) __tree:1799
   #11 0x11dc5d823 in base::SupportsUserData::~SupportsUserData() __tree:1789
   #12 0x115f302d2 in content::WebContentsImpl::~WebContentsImpl() web_contents_impl.cc:1088
   #13 0x115f3264d in content::WebContentsImpl::~WebContentsImpl() web_contents_impl.cc:990
   #14 0x1156a8a8f in content::Portal::~Portal() portal.cc:678
   #15 0x1156a8ccd in content::Portal::~Portal() portal.cc:59
   #16 0x1159fe283 in content::RenderFrameHostImpl::DestroyPortal(content::Portal*) unique_ptr.h:54
   #17 0x115fbaff4 in content::WebContentsImpl::Close(content::RenderViewHost*) web_contents_impl.cc:7180

   #18 0x115b6c9da in base::internal::Invoker<base::internal::BindState<void (content::RenderViewHostImpl::*)(),
base::WeakPtr<content::RenderViewHostImpl> >, void ()>::RunOnce(base::internal::BindStateBase*) bind_internal.h:543
   #19 0x11371f5fa in blink::mojom::LocalMainFrame_ClosePage_ForwardToCallback::Accept(mojo::Message*)
   #19 0x1137ff5fa in blink::mojom::LocalMainFrame_ClosePage_ForwardToCallback::Accept(mojo::Message*)
callback.h:142
   #20 0x11e264c8c in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
interface_endpoint_client.cc:896
   #21 0x11e272fb4 in mojo::MessageDispatcher::Accept(mojo::Message*) message_dispatcher.cc:43
   #22 0x11e268fa4 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
interface_endpoint_client.cc:658
   #23 0x11ff0a84d in IPC::(anonymous
namespace)::ChannelAssociatedGroupController::AcceptOnEndpointThread(mojo::Message) ipc_mojo_bootstrap.cc:1008
   #24 0x11ff044bc 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*)
bind_internal.h:543
   #25 0x11dc6ad0f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) callback.h:142
   #26 0x11dcaf56c in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) task_annotator.h:74
   #27 0x11dcaed66 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc:261
   #28 0x11dcb0231 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc
   #29 0x11dd94308 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:398

previously allocated by thread T0 here:
   #0 0x10d912ed0  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x46ed0) (BuildId:
b4732162098e3d0f8e0b461cd4a22043240000001000000000070a0000010b00)
   #1 0x11ca63137 in operator new(unsigned long) new.cpp:67
   #2 0x127bab18b in TabHelpers::AttachTabHelpers(content::WebContents*) tab_helpers.cc:459
   #3 0x127c86090 in non-virtual thunk to Browser::PortalWebContentsCreated(content::WebContents*) browser.cc:1809
   #4 0x1156aabb3 in content::Portal::CreateProxyAndAttachPortal() portal.cc:195
   #5 0x115a449ec in
content::RenderFrameHostImpl::CreatePortal(mojo::PendingAssociatedReceiver<blink::mojom::Portal>,
mojo::PendingAssociatedRemote<blink::mojom::PortalClient>, base::OnceCallback<void (int,
mojo::StructPtr<blink::mojom::FrameReplicationState>, base::TokenType<blink::PortalTokenTypeMarker> const&,
base::TokenType<blink::RemoteFrameTokenTypeMarker> const&, base::UnguessableToken const&)>)
render_frame_host_impl.cc:6875
   #6 0x113db3339 in content::mojom::FrameHostStubDispatch::AcceptWithResponder(content::mojom::FrameHost*,
mojo::Message*, std::__1::unique_ptr<mojo::MessageReceiverWithStatus,
std::__1::default_delete<mojo::MessageReceiverWithStatus> >) frame.mojom.cc:5963
   #7 0x11e264831 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
interface_endpoint_client.cc:863
   #8 0x11e272eda in mojo::MessageDispatcher::Accept(mojo::Message*) message_dispatcher.cc:48
   #9 0x11e268fa4 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
interface_endpoint_client.cc:658
   #10 0x11ff0a11d in IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptSyncMessage(unsigned
int, unsigned int) ipc_mojo_bootstrap.cc:1048
   #11 0x11dc6ad0f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) callback.h:142
   #12 0x11dcaf56c in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) task_annotator.h:74

   #13 0x11dcaed66 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc:261
   #14 0x11dcb0231 in non-virtual thunk to
```

```
    #14 0x11dcb0231 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc
    #15 0x11dd94308 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:398
    #16 0x11dd817f9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xda077f9)
(BuildId: 4c4c448655553144a17fee2bd4ae26b42400000010000000000b0a0000010c00)
    #17 0x11dd92c25 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:374
    #18 0x7fff9faf9e50 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(CoreFoundation:x86_64+0xa4e50) (BuildId: 51ca5ec63fcd30d188de7b20fe8af9d12400000010000000000c0a00000c0a00)
    #19 0x7fff9fadb0cb in __CFRunLoopDoSources0+0x22b (CoreFoundation:x86_64+0x860cb) (BuildId:
51ca5ec63fcd30d188de7b20fe8af9d12400000010000000000c0a00000c0a00)
    #20 0x7fff9fada5b5 in __CFRunLoopRun+0x3a5 (CoreFoundation:x86_64+0x855b5) (BuildId:
51ca5ec63fcd30d188de7b20fe8af9d12400000010000000000c0a00000c0a00)
    #21 0x7fff9fad9fb3 in CFRunLoopRunSpecific+0x1a3 (CoreFoundation:x86_64+0x84fb3) (BuildId:
51ca5ec63fcd30d188de7b20fe8af9d12400000010000000000c0a00000c0a00)
    #22 0x7fff9f038ebb in RunCurrentEventLoopInMode+0xef (HIToolbox:x86_64+0x30ebb) (BuildId:
25e0ac2627fe32e59226f4d42b25ed302400000010000000000c0a00000c0a00)
    #23 0x7fff9f038cf0 in ReceiveNextEventCommon+0x1af (HIToolbox:x86_64+0x30cf0) (BuildId:
25e0ac2627fe32e59226f4d42b25ed302400000010000000000c0a00000c0a00)
    #24 0x7fff9f038b25 in _BlockUntilNextEventMatchingListInModeWithFilter+0x46 (HIToolbox:x86_64+0x30b25) (BuildId:
25e0ac2627fe32e59226f4d42b25ed302400000010000000000c0a00000c0a00)
    #25 0x7fff9d5cda03 in _DPSNextEvent+0x45f (AppKit:x86_64+0x46a03) (BuildId:
e39cd61301043e26b424be83ced656f92400000010000000000c0a00000c0a00)
    #26 0x7fff9dd497ed in -[NSApplication(NSEvent) _nextEventMatchingEventMask:untilDate:inMode:dequeue:]+0xaeb
(AppKit:x86_64+0x7c27ed) (BuildId: e39cd61301043e26b424be83ced656f92400000010000000000c0a00000c0a00)
    #27 0x11cae7372 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke
chrome_browser_application_mac.mm:239
    #28 0x11dd817f9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (Chromium Framework:x86_64+0xda077f9)
(BuildId: 4c4c448655553144a17fee2bd4ae26b42400000010000000000b0a0000010c00)
    #29 0x11cae6f0a in -[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]
chrome_browser_application_mac.mm:238

SUMMARY: AddressSanitizer: heap-use-after-free browser_list.cc:89 in BrowserList::AddBrowser(Browser*)
Shadow bytes around the buggy address:
  0x1c0c00002af0: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x1c0c00002b00: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x1c0c00002b10: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fa
  0x1c0c00002b20: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x1c0c00002b30: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
=>0x1c0c00002b40: fd fd fd fa fa fa fa fa fd[fd]fd fd fd fd fd fd
  0x1c0c00002b50: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x1c0c00002b60: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x1c0c00002b70: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fa
  0x1c0c00002b80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c0c00002b90: 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 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
```

screen.mov
15.7 MB Download



portal.html
120 bytes View Download

url.pdf
692 bytes Download

Comment 1 by sheriffbot on Sat, Jan 29, 2022, 12:17 AM EST   Project Member

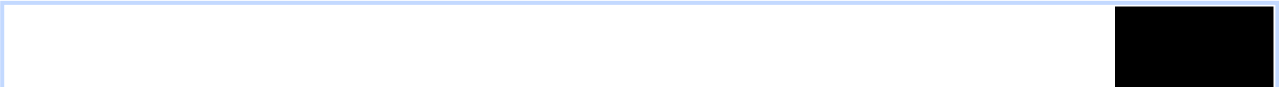
Labels: external_security_report

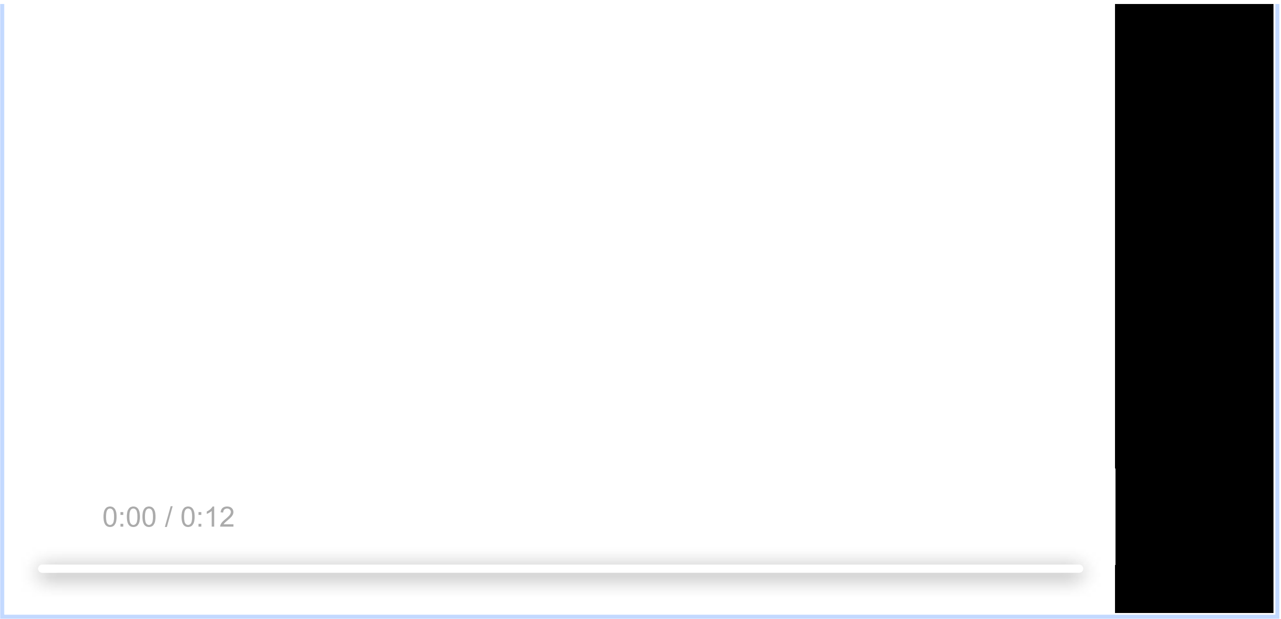
Comment 2 by chrom...@gmail.com on Sat, Jan 29, 2022, 8:59 AM EST

This doesn't affect Windows and Linux.

Please ensure that #enable-portals and #enable-portals-cross-origin from chrome://flags are enabled.

screen.mp4
10.1 MB View Download





Comment 3 by chrom...@gmail.com on Sat, Jan 29, 2022, 4:45 PM EST

I can repro this on Linux, sometimes looks like it can take several tries to repro the crash.

ASAN_Linux
20.1 KB View Download

Comment 4 by carlosil@chromium.org on Mon, Jan 31, 2022, 1:35 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: adithyas@chromium.org
Cc: carlosil@chromium.org
Labels: FoundIn-100 Security_Severity-High OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Blink>Portals

I was not able to reproduce myself, but report (and video) seem legitimate. Triageing as security high, since this is similar to ~~crbug.com/1197436~~, setting Impact-None, since this requires 2 off by default flags to be enabled. Setting all desktop OS's since reporter mentions they were able to reproduce in Linux, so it seems Mac might be the most reliable repro, but other OS's are affected.

reporter: I'm setting this as found in M100 for now since that is what you used. Could you check if this reproduces in earlier versions? Thanks

adithyas: Can you PTAL and help further triage? Feel free to reassign as appropriate. Thanks

Comment 5 by sheriffbot on Mon, Jan 31, 2022, 1:37 PM EST Project Member

Labels: Security_Impact-Head

Comment 6 by chrom...@gmail.com on Mon, Jan 31, 2022, 4:39 PM EST

I am able to repro this on stable 97.0.4692.99.

Comment 7 by carlosil@chromium.org on Mon, Jan 31, 2022, 4:40 PM EST Project Member

Labels: -FoundIn-100 FoundIn-97

Thanks for checking, adjusting the FoundIn label accordingly.

[illegible], adjusting [illegible] accordingly

Comment 8 by sheriffbot on Mon, Jan 31, 2022, 4:43 PM EST Project Member

Labels: -Security_Impact-Head Security_Impact-Stable

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.

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-3 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 sheriffbot on Sat, Feb 12, 2022, 12:21 PM EST Project Member

adithyas: 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 14 by adithyas@chromium.org on Mon, Feb 14, 2022, 3:32 PM EST Project Member

I was able to repro on Mac. This is being triggered by portal activation and is caused by a race - and is an issue in TabModalDialogManager. It looks like it is possible for JavaScriptTabModalDialogManagerDelegateDesktop to add itself as an observer of BrowserList, but not remove itself when it gets destroyed. BrowserList::RemoveObserver is called from JavaScriptTabModalDialogManagerDelegateDesktop::DidCloseDialog (and not in it's destructor)

During portal activation, we first destroy the predecessor page's RWHV - and then after some amount of time (determined by JS execution in the onportalactivate event), we destroy the predecessor's WebContents. We either run:

Portal::CloseContents -> ~TabModalDialogManager -> TabModalDialogManager::CloseDialog -> JavaScriptTabModalDialogManagerDelegateDesktop::DidCloseDialog

```
JavaScriptTabModalDialogManagerDelegateDesktop:DidCloseDialog
                                                                    -> ~JavaScriptTabModalDialogManagerDelegateDesktop
[ViewsNSWindowDelegate windowWillClose) -> ~JavaScriptTabModalDialogViewViews
```

or we run:

```
[ViewsNSWindowDelegate windowWillClose) -> ~JavaScriptTabModalDialogViewViews
Portal::CloseContents -> ~TabModalDialogManager -> TabModalDialogManager::CloseDialog  (RemoveObserver is NOT called)
                                                                    -> ~JavaScriptTabModalDialogManagerDelegateDesktop
```

TabModalDialogManager::CloseDialog checks if |dialog_| (which is a WeakPtr to a JavaScriptTabModalDialogViewViews instance) is valid. If it's invalid, it does not call DidCloseDialog which calls RemoveObserver. So in the second scenario, we have the View which is seperately destroyed before TabModalDialogManager, and because TabModalDialogManager is destroyed after, the |dialog_| pointer is invalid and TabModalDialogManager skips the code that tells the delegate that a dialog closed and that it should remove itself as an observer.

Comment 15 by adithyas@chromium.org on Mon, Feb 14, 2022, 3:32 PM EST Project Member

Components: Blink>WindowDialog

Comment 16 by adithyas@chromium.org on Mon, Feb 14, 2022, 5:38 PM EST Project Member

Weirdly though, we call RegisterWindowWillCloseCallback in JavaScriptTabModalDialogViewsView [1] to handle this case - but the callback isn't being called in this case for some reason (I'm not sure why yet). Using RegisterDeleteDelegateCallback instead seems to do the trick.

[1] https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/javascript_tab_modal_dialog_view_views.cc;l=93;drc=0fd3cccdbb7ee1e0ff1abd76c15956a9c4c3fbae

Comment 17 by adithyas@chromium.org on Wed, Feb 23, 2022, 5:52 PM EST Project Member

Labels: Pri-3

I'm reasonably sure that this can only be reproed with portals, so lowering priority. Seems like the best way to resolve this is to just close all modal dialogs before activation - this will force the dialog to close and the observer to be cleaned up before we destroy the RWHV after activation.

Comment 18 by adithyas@chromium.org on Fri, Feb 25, 2022, 9:17 AM EST Project Member

Cc: mcnee@chromium.org

Comment 19 by Git Watcher on Fri, Feb 25, 2022, 1:29 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2f06825c8a968f2c9b0e1391cfa9f4eef984f261

commit 2f06825c8a968f2c9b0e1391cfa9f4eef984f261
Author: Adithya Srinivasan <adithyas@chromium.org>
Date: Fri Feb 25 18:28:35 2022

Fix UAF in JavaScriptTabModalDialogManagerDelegateDesktop

See bug for more details.

~~Bug: 1292261~~
Change-Id: Iebe499b4eda76b1b190f5f7b97a0938eb22dc405
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3465258
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Adithya Srinivasan <adithyas@chromium.org>
Cr-Commit-Position: refs/heads/main@{#975178}

[modify] https://crrev.com/2f06825c8a968f2c9b0e1391cfa9f4eef984f261/content/browser/portal/portal.cc

Comment 20 by chrom...@gmail.com on Fri, Feb 25, 2022, 3:08 PM EST

Thanks for the fix!

Comment 21 by adithyas@chromium.org on Mon, Feb 28, 2022, 9:57 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 22 by sheriffbot on Mon, Feb 28, 2022, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 23 by sheriffbot on Tue, Mar 1, 2022, 1:41 PM EST Project Member

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

Comment 24 by sheriffbot on Tue, Mar 1, 2022, 2:02 PM EST Project Member

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

Requesting merge to stable M98 because latest trunk commit (975178) appears to be after stable branch point (950365).

Requesting merge to beta M99 because latest trunk commit (975178) appears to be after beta branch point (961656).

Requesting merge to dev M100 because latest trunk commit (975178) appears to be after dev branch point (972766).

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

Comment 25 by sheriffbot on Tue, Mar 1, 2022, 2:03 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 26 by sheriffbot on Tue, Mar 1, 2022, 2:03 PM EST Project Member

Labels: -Merge-Request-99 Merge-Reject-99 Hotlist-Merge-Reject

Merge rejected: M99 is already shipping to stable and this issue is marked as a Pri-2, Pri-3, or Type-Feature.

Please contact the milestone owner if you have questions.

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 27 by sheriffbot on Tue, Mar 1, 2022, 2:03 PM EST Project Member

Labels: -Merge-Request-98 Merge-Reject-98

Merge rejected: M98 is already shipping to stable and this issue is marked as a Pri-2, Pri-3, or Type-Feature.

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 28 by sheriffbot on Mon, Mar 7, 2022, 12:22 PM EST Project Member

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

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

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

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

Comment 29 by srinivassista@google.com on Mon, Mar 7, 2022, 2:55 PM EST Project Member

This bug is approved for M100 merge, please complete your merge asap so this can be included in the beta release this week. Beta RC will be cut tomorrow (tuesday) March 8th at 3pm PST [Bulk Update]

Comment 30 by Git Watcher on Mon, Mar 7, 2022, 3:13 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/+/327b900d80bdb717d697cc0766b88bdfe230a1e8

commit 327b900d80bdb717d697cc0766b88bdfe230a1e8
Author: Adithya Srinivasan <adithyas@chromium.org>
Date: Mon Mar 07 20:12:02 2022

Fix UAF in JavaScriptTabModalDialogManagerDelegateDesktop

See bug for more details.

(cherry picked from commit 2f06825c8a968f2c9b0e1391cfa9f4eef984f261)

~~Bug: 1292261~~
Change-Id: Iebe499b4eda76b1b190f5f7b97a0938eb22dc405
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3465258
Reviewed-by: Kevin McNee <mcnee@chromium.org>
Commit-Queue: Adithya Srinivasan <adithyas@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#975178}

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3507975
Auto-Submit: Adithya Srinivasan <adithyas@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4896@{#344}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify] https://crrev.com/327b900d80bdb717d697cc0766b88bdfe230a1e8/content/browser/portal/portal.cc

Comment 31 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 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 32 by amyressler@chromium.org on Thu, Mar 10, 2022, 10:48 PM EST Project Member

Congratulations, Khalil, 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 33 by amyressler@google.com on Fri, Mar 11, 2022, 2:44 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 34 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:56 PM EDT Project Member

Labels: Release-0-M100

Comment 35 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

Labels: CVE-2022-1125 CVE_description-missing

Comment 36 by gmpritchard@google.com on Thu, Mar 31, 2022, 11:43 AM EDT Project Member

Labels: LTS-NotApplicable-96

Comment 37 by gmpritchard@google.com on Thu, Mar 31, 2022, 11:50 AM EDT Project Member

Labels: -LTS-NotApplicable-96 LTS-Merge-Candidate

Comment 38 by voit@google.com on Tue, Apr 5, 2022, 4:12 AM EDT Project Member

Labels: LTS-Evaluating-96

Comment 39 by voit@google.com on Tue, Apr 5, 2022, 9:26 AM EDT Project Member

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

Comment 40 by sheriffbot on Tue, Apr 5, 2022, 9:35 AM EDT Project Member

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

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

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

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

Comment 41 by voit@google.com on Tue, Apr 5, 2022, 10:48 AM EDT Project Member

1. https://crrev.com/c/3570850
2. Low - small changes, no conflicts
3. M100
4. Yes

Comment 42 by gmpritchard@google.com on Wed, Apr 6, 2022, 5:40 PM EDT Project Member

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

Comment 43 by Git Watcher on Thu, Apr 7, 2022, 1:16 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/591d198d2e38e017bcde793deb87c2e694cf282a

commit 591d198d2e38e017bcde793deb87c2e694cf282a
Author: Adithya Srinivasan <adithyas@chromium.org>
Date: Thu Apr 07 17:15:05 2022

[M96-LTS] Fix UAF in JavaScriptTabModalDialogManagerDelegateDesktop

See bug for more details.

(cherry picked from commit 2f06825c8a968f2c9b0e1391cfa9f4eef984f261)

(cherry picked from commit 327b900d80bdb717d697cc0766b88bdfe230a1e8)

~~Bug: 1292261~~
Change-Id: Iebe499b4eda76b1b190f5f7b97a0938eb22dc405
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3465258
Commit-Queue: Adithya Srinivasan <adithyas@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/main@{#975178}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3507975
Auto-Submit: Adithya Srinivasan <adithyas@chromium.org>

Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Original-Commit-Position: refs/branch-heads/4896@{#344}

Cr-Original-Commit-Position: refs/branch-heads/4896@{#344}
Cr-Original-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3570850
Reviewed-by: Simon Hangl <simonha@google.com>
Owners-Override: Simon Hangl <simonha@google.com>
Commit-Queue: Zakhar Voit <voit@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1577}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/591d198d2e38e017bcde793deb87c2e694cf282a/content/browser/portal/portal.cc

Comment 44 by voit@google.com on Fri, Apr 8, 2022, 4:38 AM EDT Project Member

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

Comment 45 by sheriffbot on Mon, Jun 6, 2022, 1:32 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 46 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 47 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing