Starred by 3 users

| | |
|---|---|
| **Owner:** | maxlg@chromium.org<br>**Last visit > 30 days ago** |
| **CC:** | a...@chromium.org<br>nburris@chromium.org<br>adetaylor@chromium.org<br>smcgruer@chromium.org<br>rouslan@chromium.org<br>danyao@chromium.org<br>robliao@chromium.org<br>maxlg@chromium.org<br>pbomm...@chromium.org<br>wittman@chromium.org |
| **Status:** | Fixed *(Closed)* |
| **Components:** | Blink>Payments |
| **Modified:** | Aug 19, 2021 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Windows, Chrome |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
Build-Official
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
M-90
Target-90
merge-merged-4240
Web-Payments-ZBB
LTS-Security-86
external_security_report
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4472

## Issue 1194058: Security: heap-use-after-free in the payment dialog in the browser process

Reported by 0xasn...@gmail.com on Tue, Mar 30, 2021, 9:22 AM EDT

Code

Description #8 by maxlg@chromium.org (Apr 26, 2021)

**VULNERABILITY DETAILS**
heap-use-after-free in the payment dialog in the browser process which will excape the sandbox.

**VERSION**
Chrome Version: [91.0.4464.0] + [dev] (asan-win32-release_x64-867481) (not reproducible on official releases)
- Download: https://commondatastorage.googleapis.com/chromium-browser-asan/index.html?prefix=linux-release/asan-linux-release-867878
- other reproducible versions: 87.0.4258.0
- The "showDirectoryPicker" API was introduced in 86

Operating System: Windows 10 , Linux

**REPRODUCTION CASE**

You can see the gif poc directly~

Prepare:
1. open https://skilful-reserve-239412.appspot.com/static/apps/navigation-tester/ and install
2. open https://skilful-reserve-239412.appspot.com/static/apps/max-nonbasiccard/ and install
3. open https://maxlgu.github.io/pr/max-nonbasiccard/ and click Buy
4. Navigate to a Dialog pop up Page and then click the Back button ,Boom

maxlg@: an easier reproduction method - #c40

Reprodeuce Method 1(The easier one, Set the chromimu display language as Chinese (maxlg@: unnecessary info)):
See the poc1.gif

Reprodeuce Method 2:
Open the popup.html in the navigate textarea and click go.
Select the default folder and select ok.
Click the Back button
See the poc2.gif

**FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION**
Type of crash: [ browser]

```
F:\20210330 POC\asan-win32-release_x64-867481>chrome.exe --user-data-dir=c:/tmp/noexist
=================================================================
==1768==ERROR: AddressSanitizer: heap-use-after-free on address 0x114a19856fb0 at pc 0x7ffa08e4fc60 bp 0x0020fcbfc550 sp 0x0020fcbfc598
READ of size 8 at 0x114a19856fb0 thread T0
==1768==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ffa08e4fc5f in web_modal::WebContentsModalDialogManager::BlockWebContentsInteraction
C:\b\s\w\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc:116
    #1 0x7ffa08e4ff66 in web_modal::WebContentsModalDialogManager::WillClose
```

C:\b\s\w\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc:82
    #2 0x7ffa1357ebb6 in constrained_window::NativeWebContentsModalDialogManagerViews::WidgetClosing
C:\b\s\w\ir\cache\builder\src\components\constrained_window\native_web_contents_modal_dialog_manager_views.cc:226
    #3 0x7ffa06b27b34 in views::Widget::CloseWithReason C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:635
    #4 0x7ffa08e5065c in web_modal::WebContentsModalDialogManager::CloseAllDialogs
C:\b\s\w\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc:124
    #5 0x7ffa014212b1 in content::WebContentsImpl::WebContentsObserverList::NotifyObservers<void (content::WebContentsObserver::*)()>
C:\b\s\w\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.h:1425
    #6 0x7ffa0141eea5 in content::WebContentsImpl::~WebContentsImpl C:\b\s\w\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc:961
    #7 0x7ffa01492fab in content::WebContentsImpl::~WebContentsImpl C:\b\s\w\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc:889
    #8 0x7ffa108e5d28 in views::WebView::SetWebContents C:\b\s\w\ir\cache\builder\src\ui\views\controls\webview\webview.cc:94
    #9 0x7ffa108e5b80 in views::WebView::~WebView C:\b\s\w\ir\cache\builder\src\ui\views\controls\webview\webview.cc:71
    #10 0x7ffa108e949b in views::WebView::~WebView C:\b\s\w\ir\cache\builder\src\ui\views\controls\webview\webview.cc:69
    #11 0x7ffa06af4e40 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:238
    #12 0x7ffa06b1b533 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:211
    #13 0x7ffa06af4e40 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:238
    #14 0x7ffa06b1b533 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:211
    #15 0x7ffa06af4e40 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:238
    #16 0x7ffa06b1b533 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:211
    #17 0x7ffa06af4e40 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:238
    #18 0x7ffa09312c31 in views::ScrollView::~ScrollView C:\b\s\w\ir\cache\builder\src\ui\views\controls\scroll_view.cc:246
    #19 0x7ffa06af4e40 in views::View::~View C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:238
    #20 0x7ffa16680376 in payments::`anonymous namespace'::SheetView::~SheetView
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc:52
    #21 0x7ffa16679a4e in ViewStack::Pop C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\view_stack.cc:76
    #22 0x7ffa155dad6b in payments::PaymentRequestDialogView::GoBack
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_dialog_view.cc:264
    #23 0x7ffa1667fef6 in payments::PaymentRequestSheetController::BackButtonPressed
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc:532
    #24 0x7ffa06ae8155 in base::internal::Invoker<base::internal::BindState<`lambda at ../../ui/views/controls/button/button.cc:101:31',base::RepeatingCallback<void ()> >,void
(const ui::Event &)>::Run C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:703
    #25 0x7ffa092d6b62 in views::ButtonController::OnMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\controls\button\button_controller.cc:58
    #26 0x7ffa06b09580 in views::View::ProcessMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:3019
    #27 0x7ffa079e0820 in ui::EventHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37
    #28 0x7ffa0ffd1476 in ui::ScopedTargetHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\scoped_target_handler.cc:28
    #29 0x7ffa079df103 in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:191
    #30 0x7ffa079de623 in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:140
    #31 0x7ffa079de00c in ui::EventDispatcherDelegate::DispatchEventToTarget C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:84
    #32 0x7ffa079ddc50 in ui::EventDispatcherDelegate::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:56
    #33 0x7ffa0932d32d in views::internal::RootView::OnMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\widget\root_view.cc:480
    #34 0x7ffa06b3007b in views::Widget::OnMouseEvent C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1330
    #35 0x7ffa079e0820 in ui::EventHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37
    #36 0x7ffa079df103 in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:191
    #37 0x7ffa079de623 in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:140
    #38 0x7ffa079de00c in ui::EventDispatcherDelegate::DispatchEventToTarget C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:84
    #39 0x7ffa079ddc50 in ui::EventDispatcherDelegate::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:56
    #40 0x7ffa0c1d939c in ui::EventProcessor::OnEventFromSource C:\b\s\w\ir\cache\builder\src\ui\events\event_processor.cc:49
    #41 0x7ffa0931c36f in ui::EventSource::DeliverEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:113
    #42 0x7ffa0931bfc9 in ui::EventSource::SendEventToSinkFromRewriter C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:138
    #43 0x7ffa0931bac7 in ui::EventSource::SendEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:107
    #44 0x7ffa0c1d61fd in views::DesktopWindowTreeHostWin::HandleMouseEvent
C:\b\s\w\ir\cache\builder\src\ui\views\widget\desktop_aura\desktop_window_tree_host_win.cc:958
    #45 0x7ffa10024f31 in views::HWNDMessageHandler::HandleMouseEventInternal C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:3140
    #46 0x7ffa1001e373 in views::HWNDMessageHandler::_ProcessWindowMessage C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.h:355
    #47 0x7ffa1001dae2 in views::HWNDMessageHandler::OnWndProc C:\b\s\w\ir\cache\builder\src\ui\views\win\hwnd_message_handler.cc:1012
    #48 0x7ffa09a78e96 in gfx::WindowImpl::WndProc C:\b\s\w\ir\cache\builder\src\ui\gfx\win\window_impl.cc:305
    #49 0x7ffa09a777b1 in base::win::WrappedWindowProc<&gfx::WindowImpl::WndProc> C:\b\s\w\ir\cache\builder\src\base\win\wrapped_window_proc.h:74
    #50 0x7ffa8d06e857 in CallWindowProcW+0x3f7 (C:\WINDOWS\System32\user32.dll+0x18000e857)
    #51 0x7ffa8d06e298 in DispatchMessageW+0x258 (C:\WINDOWS\System32\user32.dll+0x18000e298)
    #52 0x7ffa06d70b34 in base::MessagePumpForUI::ProcessMessageHelper C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:537
    #53 0x7ffa06d6edbd in base::MessagePumpForUI::ProcessNextWindowsMessage C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:500
    #54 0x7ffa06d6e69c in base::MessagePumpForUI::DoRunLoop C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:215
    #55 0x7ffa06d6c928 in base::MessagePumpWin::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #56 0x7ffa094360bf in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460
    #57 0x7ffa06c43483 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:133
    #58 0x7ffa005ed4fc in content::BrowserMainLoop::RunMainMessageLoop C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:991
    #59 0x7ffa005f297f in content::BrowserMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:150
    #60 0x7ffa005e68b2 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:47
    #61 0x7ffa069f38b0 in content::RunBrowserProcessMain C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:582
    #62 0x7ffa069f61a8 in content::ContentMainRunnerImpl::RunBrowser C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1062
    #63 0x7ffa069f5445 in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:940
    #64 0x7ffa069f2732 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:372
    #65 0x7ffa069f2d1c in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:398
    #66 0x7ff9fcc5145a in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:141
    #67 0x7ff625e35bd5 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #68 0x7ff625e32bf9 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:369
    #69 0x7ff626215cff in __scrt_common_main_seh d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #70 0x7ffa8dc27033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #71 0x7ffa8e042650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

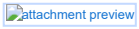
0x114a19856fb0 is located 368 bytes inside of 392-byte region [0x114a19856e40,0x114a19856fc8)
freed by thread T0 here:
    #0 0x7ff625ed27fb in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffa16684f3d in payments::PaymentHandlerWebFlowViewController::~PaymentHandlerWebFlowViewController
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_handler_web_flow_view_controller.cc:218
    #2 0x7ff9ffbcf804 in std::__1::__tree<std::__value_type<unsigned int,std::unique_ptr<gpu::gles2::AbstractTexture,std::default_delete<gpu::gles2::AbstractTexture> >
>,std::__map_value_compare<unsigned int,std::__value_type<unsigned int,std::unique_ptr<gpu::gles2::AbstractTexture,std::default_delete<gpu::gles2::AbstractTexture> >
>,std::less<unsigned int>,1>,std::allocator<std::__value_type<unsigned int,std::unique_ptr<gpu::gles2::AbstractTexture,std::default_delete<gpu::gles2::AbstractTexture> > > >
>::erase C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree:2422
    #3 0x7ffa155df744 in std::__1::__tree<std::__value_type<views::View
*,std::unique_ptr<payments::PaymentRequestSheetController,std::default_delete<payments::PaymentRequestSheetController> > >,std::__map_value_compare<views::View
*,std::__value_type<views::View *,std::unique_ptr<payments::PaymentRequestSheetController,std::default_delete<payments::PaymentRequestSheetController> >
>,std::less<views::View *>,1>,std::allocator<std::__value_type<views::View
*,std::unique_ptr<payments::PaymentRequestSheetController,std::default_delete<payments::PaymentRequestSheetController> > > >::__erase_unique<views::View *>
C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include__tree:2445
    #4 0x7ffa06b1472b in views::View::ViewHierarchyChangedImpl C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:2647
    #5 0x7ffa06b15669 in views::View::PropagateRemoveNotifications C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:2602
    #6 0x7ffa06af6b2c in views::View::DoRemoveChildView C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:2567
    #7 0x7ffa06af5823 in views::View::RemoveChildView C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:302
    #8 0x7ffa16679a0c in ViewStack::Pop C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\view_stack.cc:76
    #9 0x7ffa155dad6b in payments::PaymentRequestDialogView::GoBack
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_dialog_view.cc:264

```
    #10 0x7ffa1667fef6 in payments::PaymentRequestSheetController::BackButtonPressed
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc:532
    #11 0x7ffa06ae8155 in base::internal::Invoker<base::internal::BindState<`lambda at ../../ui/views/controls/button/button.cc:101:31',base::RepeatingCallback<void ()> >,void
(const ui::Event &)>::Run C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:703
    #12 0x7ffa092d6b62 in views::ButtonController::OnMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\controls\button\button_controller.cc:58
    #13 0x7ffa06b09580 in views::View::ProcessMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\view.cc:3019
    #14 0x7ffa079e0820 in ui::EventHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37
    #15 0x7ffa0ffd1476 in ui::ScopedTargetHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\scoped_target_handler.cc:28
    #16 0x7ffa079df103 in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:191
    #17 0x7ffa079de623 in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:140
    #18 0x7ffa079de00c in ui::EventDispatcherDelegate::DispatchEventToTarget C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:84
    #19 0x7ffa079ddc50 in ui::EventDispatcherDelegate::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:56
    #20 0x7ffa0932d32d in views::internal::RootView::OnMouseReleased C:\b\s\w\ir\cache\builder\src\ui\views\widget\root_view.cc:480
    #21 0x7ffa06b3007b in views::Widget::OnMouseEvent C:\b\s\w\ir\cache\builder\src\ui\views\widget\widget.cc:1330
    #22 0x7ffa079e0820 in ui::EventHandler::OnEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_handler.cc:37
    #23 0x7ffa079df103 in ui::EventDispatcher::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:191
    #24 0x7ffa079de623 in ui::EventDispatcher::ProcessEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:140
    #25 0x7ffa079de00c in ui::EventDispatcherDelegate::DispatchEventToTarget C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:84
    #26 0x7ffa079ddc50 in ui::EventDispatcherDelegate::DispatchEvent C:\b\s\w\ir\cache\builder\src\ui\events\event_dispatcher.cc:56
    #27 0x7ffa0c1d939c in ui::EventProcessor::OnEventFromSource C:\b\s\w\ir\cache\builder\src\ui\events\event_processor.cc:49
    #28 0x7ffa0931c36f in ui::EventSource::DeliverEventToSink C:\b\s\w\ir\cache\builder\src\ui\events\event_source.cc:113

previously allocated by thread T0 here:
    #0 0x7ff625ed28fb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffa18fc662a in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffa155d8217 in payments::PaymentRequestDialogView::ShowPaymentHandlerScreen
C:\b\s\w\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_dialog_view.cc:169
    #3 0x7ffa13acd501 in payments::ChromePaymentRequestDelegate::EmbedPaymentHandlerWindow
C:\b\s\w\ir\cache\builder\src\chrome\browser\payments\chrome_payment_request_delegate.cc:243
    #4 0x7ffa096cb0df in payments::PaymentRequestDisplayManager::ShowPaymentHandlerWindow
C:\b\s\w\ir\cache\builder\src\components\payments\content\payment_request_display_manager.cc:65
    #5 0x7ffa0701eef6 in ChromeContentBrowserClient::ShowPaymentHandlerWindow C:\b\s\w\ir\cache\builder\src\chrome\browser\chrome_content_browser_client.cc:5365
    #6 0x7ffa011c2113 in content::`anonymous namespace'::ShowPaymentHandlerWindowOnUI
C:\b\s\w\ir\cache\builder\src\content\browser\service_worker\payment_handler_support.cc:83
    #7 0x7ffa011c3669 in base::internal::Invoker<base::internal::BindState<void (*)(scoped_refptr<content::ServiceWorkerContextWrapper>, const GURL &,
base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string> &)>, bool, int, int)>,
base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string> &)>)>,
base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string>
&)>),scoped_refptr<content::ServiceWorkerContextWrapper>,GURL,base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string> &)>, bool, int, int)>,base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string> &)>)>,base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, const base::Optional<std::string> &)> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #8 0x7ffa00109c0a in content::RunOrPostTaskOnThread C:\b\s\w\ir\cache\builder\src\content\public\browser\browser_thread.cc:20
    #9 0x7ffa011c1c81 in content::PaymentHandlerSupport::ShowPaymentHandlerWindow
C:\b\s\w\ir\cache\builder\src\content\browser\service_worker\payment_handler_support.cc:103
    #10 0x7ffa01323cb6 in content::ServiceWorkerVersion::OpenPaymentHandlerWindow
C:\b\s\w\ir\cache\builder\src\content\browser\service_worker\service_worker_version.cc:1422
    #11 0x7ff9ff442da3 in blink::mojom::ServiceWorkerHostStubDispatch::AcceptWithResponder
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\third_party\blink\public\mojom\service_worker\service_worker.mojom.cc:2221
    #12 0x7ffa0132cf7e in blink::mojom::ServiceWorkerHostStub<mojo::RawPtrImplRefTraits<blink::mojom::ServiceWorkerHost> >::AcceptWithResponder
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\third_party\blink\public\mojom\service_worker\service_worker.mojom.h:450
    #13 0x7ffa0710f57b in mojo::InterfaceEndpointClient::HandleValidatedMessage C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:526
    #14 0x7ffa09861096 in mojo::MessageDispatcher::Accept C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #15 0x7ffa07120d79 in mojo::internal::MultiplexRouter::ProcessIncomingMessage C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:955
    #16 0x7ffa0711fe48 in mojo::internal::MultiplexRouter::Accept C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:622
    #17 0x7ffa09861096 in mojo::MessageDispatcher::Accept C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #18 0x7ffa0710a3d6 in mojo::Connector::DispatchMessageW C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:508
    #19 0x7ffa0710bb2b in mojo::Connector::ReadAllAvailableMessages C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\connector.cc:566
    #20 0x7ffa07158a3d in mojo::SimpleWatcher::OnHandleReady C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\system\simple_watcher.cc:278
    #21 0x7ffa06cbd4c7 in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:173
    #22 0x7ffa09434ac7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:351
    #23 0x7ffa094341a9 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:264
    #24 0x7ffa06d6e740 in base::MessagePumpForUI::DoRunLoop C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #25 0x7ffa06d6c928 in base::MessagePumpWin::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #26 0x7ffa094360bf in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460
    #27 0x7ffa06c43483 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:133
    #28 0x7ffa005ed4fc in content::BrowserMainLoop::RunMainMessageLoop C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:991

SUMMARY: AddressSanitizer: heap-use-after-free C:\b\s\w\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc:116 in
web_modal::WebContentsModalDialogManager::BlockWebContentsInteraction
Shadow bytes around the buggy address:
  0x034b5c90ada0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x034b5c90adb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x034b5c90adc0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x034b5c90add0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x034b5c90ade0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x034b5c90adf0: fd fd fd fd fd fd[fd]fd fd fa fa fa fa fa fa fa
  0x034b5c90ae00: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x034b5c90ae10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x034b5c90ae20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x034b5c90ae30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa
  0x034b5c90ae40: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
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
==1768==ABORTING

**poc1.gif**
9.6 MB View Download


**poc2.gif**
7.1 MB View Download


**popup.html**
227 bytes View Download

**asan.txt**
22.0 KB View Download

Comment 1 by sheriffbot on Tue, Mar 30, 2021, 9:24 AM EDT

**Labels:** external_security_report

Comment 2 by drubery@chromium.org on Wed, Mar 31, 2021, 2:53 PM EDT

**Status:** Assigned (was: Unconfirmed)
**Owner:** maxlg@chromium.org
**Cc:** danyao@chromium.org
**Labels:** Security_Severity-Medium Security_Impact-Stable Build-Official OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
**Components:** Blink>Payments

I was not able to reproduce the crash, but in a build with DCHECK enabled, we do fail a DCHECK. I'm not clear on the security implications of this particular DCHECK. Since it requires significant user interaction, especially within the payment handler, triaging as medium severity.

The DCHECK failure:
[2346009:2346009:0331/111333.540103:FATAL:payment_handler_web_flow_view_controller.cc(367)] Check failed: navigation_handle->HasCommitted(
    #0 0x55b0515284bb in backtrace /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:4205:13
    #1 0x7fd3d1a61389 in base::debug::CollectStackTrace(void**, unsigned long) ./../../base/debug/stack_trace_posix.cc:833:39
    #2 0x7fd3d169d223 in StackTrace ./../../base/debug/stack_trace.cc:198:12
    #3 0x7fd3d169d223 in base::debug::StackTrace::StackTrace() ./../../base/debug/stack_trace.cc:195:28
    #4 0x7fd3d171b430 in logging::LogMessage::~LogMessage() ./../../base/logging.cc:565:29
    #5 0x7fd3d171d28e in logging::LogMessage::~LogMessage() ./../../base/logging.cc:559:27
    #6 0x55b05aee69c3 in payments::PaymentHandlerWebFlowViewController::DidFinishNavigation(content::NavigationHandle*)
./../../chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc:367:3
    #7 0x7fd3c5ec3c4a in void content::WebContentsImpl::WebContentsObserverList::NotifyObservers<void (content::WebContentsObserver::*)
(content::NavigationHandle*), content::NavigationHandle*&>(void (content::WebContentsObserver::*)(content::NavigationHandle*), content::NavigationHandle*&)
./../../content/browser/web_contents/web_contents_impl.h:1425:9
    #8 0x7fd3c5ec4c31 in content::WebContentsImpl::DidFinishNavigation(content::NavigationHandle*) ./../../content/browser/web_contents/web_contents_impl.cc:5210:16
    #9 0x7fd3c56e2733 in content::NavigationRequest::~NavigationRequest() ./../../content/browser/renderer_host/navigation_request.cc:1408:20
    #10 0x7fd3c56e4d7e in content::NavigationRequest::~NavigationRequest() ./../../content/browser/renderer_host/navigation_request.cc:1367:41
    #11 0x7fd3c5486ded in operator() ./../../buildtools/third_party/libc++/trunk/include/memory:1335:5
    #12 0x7fd3c5486ded in reset ./../../buildtools/third_party/libc++/trunk/include/memory:1596:7
    #13 0x7fd3c5486ded in content::FrameTreeNode::ResetNavigationRequest(bool) ./../../content/browser/renderer_host/frame_tree_node.cc:551:23
    #14 0x7fd3c56e859f in MaybeCancelFailedNavigation ./../../content/browser/renderer_host/navigation_request.cc:6170:23
    #15 0x7fd3c56e859f in content::NavigationRequest::OnRequestFailedInternal(network::URLLoaderCompletionStatus const&, bool,
base::Optional<std::__Cr::basic_string<char, std::__Cr::char_traits<char>, std::__Cr::allocator<char> > > const&, bool)
./../../content/browser/renderer_host/navigation_request.cc:3078:7
    #16 0x7fd3c5708387 in content::NavigationRequest::OnRequestFailed(network::URLLoaderCompletionStatus const&)
./../../content/browser/renderer_host/navigation_request.cc:3039:3
    #17 0x7fd3c50e3fe8 in content::NavigationURLLoaderImpl::NotifyRequestFailed(network::URLLoaderCompletionStatus const&)
./../../content/browser/loader/navigation_url_loader_impl.cc:1317:14
    #18 0x7fd3c50f0b97 in Invoke<void (content::NavigationURLLoaderImpl::*)(const network::URLLoaderCompletionStatus &),
base::WeakPtr<content::NavigationURLLoaderImpl>, network::URLLoaderCompletionStatus> ./../../base/bind_internal.h:509:12
    #19 0x7fd3c50f0b97 in MakeItSo<void (content::NavigationURLLoaderImpl::*)(const network::URLLoaderCompletionStatus &),
base::WeakPtr<content::NavigationURLLoaderImpl>, network::URLLoaderCompletionStatus> ./../../base/bind_internal.h:668:5
    #20 0x7fd3c50f0b97 in RunImpl<void (content::NavigationURLLoaderImpl::*)(const network::URLLoaderCompletionStatus &),
std::tuple<base::WeakPtr<content::NavigationURLLoaderImpl>, network::URLLoaderCompletionStatus>, 0, 1> ./../../base/bind_internal.h:721:12
    #21 0x7fd3c50f0b97 in base::internal::Invoker<base::internal::BindState<void (content::NavigationURLLoaderImpl::*)(network::URLLoaderCompletionStatus const&),
base::WeakPtr<content::NavigationURLLoaderImpl>, network::URLLoaderCompletionStatus>, void ()>::RunOnce(base::internal::BindStateBase*)
./../../base/bind_internal.h:690:12
    #22 0x7fd3d18df9e5 in Run ./../../base/callback.h:101:12
    #23 0x7fd3d18df9e5 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:173:33
    #24 0x7fd3d1951748 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #25 0x7fd3d19504fc in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #26 0x7fd3d174a4aa in HandleDispatch ./../../base/message_loop/message_pump_glib.cc:374:46
    #27 0x7fd3d174a4aa in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) ./../../base/message_loop/message_pump_glib.cc:124:43
    #28 0x7fd377c30e6b in g_main_context_dispatch ??:0:0
    #29 0x7fd377c31118 in g_main_context_dispatch ??:?
    #30 0x7fd377c31118 in ?? ??:0
    #31 0x7fd377c311cf in g_main_context_iteration ??:0:0
    #32 0x7fd3d1749048 in base::MessagePumpGlib::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_glib.cc:400:30
    #33 0x7fd3d1953484 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460:12
    #34 0x7fd3d182f38a in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133:14
    #35 0x7fd3c4788999 in content::BrowserMainLoop::RunMainMessageLoop() ./../../content/browser/browser_main_loop.cc:986:20
    #36 0x7fd3c478e37d in content::BrowserMainRunnerImpl::Run() ./../../content/browser/browser_main_runner_impl.cc:150:15
    #37 0x7fd3c478166b in content::BrowserMain(content::MainFunctionParams const&) ./../../content/browser/browser_main.cc:47:28
    #38 0x7fd3c701774b in RunBrowserProcessMain ./../../content/app/content_main_runner_impl.cc:582:10
    #39 0x7fd3c701774b in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) ./../../content/app/content_main_runner_impl.cc:1062:10
    #40 0x7fd3c7016998 in content::ContentMainRunnerImpl::Run(bool) ./../../content/app/content_main_runner_impl.cc:940:12
    #41 0x7fd3c700f315 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) ./../../content/app/content_main.cc:372:36
    #42 0x7fd3c700f82d in content::ContentMain(content::ContentMainParams const&) ./../../content/app/content_main.cc:398:10
    #43 0x55b051599566 in ChromeMain ./../../chrome/app/chrome_main.cc:141:12
    #44 0x7fd377364d0a in __libc_start_main ./csu/../csu/libc-start.c:308:16
    #45 0x55b0514f1eea in _start ??:0:0

Comment 3 by maxlg@chromium.org on Wed, Mar 31, 2021, 3:13 PM EDT

**Status:** Duplicate (was: Assigned)
**Mergedinto:** 1166214

Comment 4 by maxlg@chromium.org on Wed, Mar 31, 2021, 3:16 PM EDT

**Status:** Assigned (was: Duplicate)

The attached text file shows a stack trace different from #c2.

Comment 5 by 0xasn...@gmail.com on Wed, Mar 31, 2021, 6:26 PM EDT

I can reproduce this UAF issue stably in the different last asan version in the different Windows OS.
To trigger this issue, you have to install two payments service work ,that is the key.

Comment 6 by maxlg@chromium.org on Wed, Mar 31, 2021, 6:56 PM EDT

Description was changed.

Comment 7 by maxlg@chromium.org on Wed, Mar 31, 2021, 6:56 PM EDT

Adding the stack trace to the description for the ease of search.

Comment 8 by maxlg@chromium.org on Wed, Mar 31, 2021, 7:16 PM EDT

**Labels:** -OS-Mac

The crash of #c2 was due to 1166214.

Tried it on Canary 91.0.4464.2 with MacOS, with language being English, failed to reproduce.

Comment 9 by maxlg@chromium.org on Wed, Mar 31, 2021, 11:13 PM EDT

Tried it on Canary 91.0.4464.5 on Windoes 8.1, with language being Chinese, but I failed to reproduce.

Haven't tried asan yet.

Comment 10 by 0xasn...@gmail.com on Wed, Mar 31, 2021, 11:15 PM EDT

I can also reproduce this issue in the Linux.

The Asan Log:
xxx@xxx-virtual-machine:~/chromium_version/asan-linux-release-861920$ ./chrome --user-data-dir=/tmp/hehe123

```
Fontconfig error: Cannot load default config file: No such file: (null)
=================================================================
==137616==ERROR: AddressSanitizer: heap-use-after-free on address 0x614000310bb0 at pc 0x5580df8aa9ba bp 0x7fffeb6f9e60 sp 0x7fffeb6f9e58
READ of size 8 at 0x614000310bb0 thread T0 (chrome)
    #0 0x5580df8aa9b9 in BlockWebContentsInteraction components/web_modal/web_contents_modal_dialog_manager.cc:116:16
    #1 0x5580df8aa9b9 in web_modal::WebContentsModalDialogManager::WillClose(aura::Window*)
components/web_modal/web_contents_modal_dialog_manager.cc:82:3
    #2 0x5580e275f38f in constrained_window::NativeWebContentsModalDialogManagerViews::WidgetClosing(views::Widget*)
components/constrained_window/native_web_contents_modal_dialog_manager_views.cc:226:21
    #3 0x5580e096f1f9 in views::Widget::CloseWithReason(views::Widget::ClosedReason) ui/views/widget/widget.cc:634:14
    #4 0x5580df8ab81f in CloseAllDialogs components/web_modal/web_contents_modal_dialog_manager.cc:124:37
    #5 0x5580df8ab81f in WebContentsDestroyed components/web_modal/web_contents_modal_dialog_manager.cc:171:3
    #6 0x5580df8ab81f in non-virtual thunk to web_modal::WebContentsModalDialogManager::WebContentsDestroyed()
components/web_modal/web_contents_modal_dialog_manager.cc
    #7 0x5580cfa2f831 in void content::WebContentsImpl::WebContentsObserverList::NotifyObservers<void (content::WebContentsObserver::*)()>(void
(content::WebContentsObserver::*)()) content/browser/web_contents/web_contents_impl.h:1429:9
    #8 0x5580cfa2bb57 in content::WebContentsImpl::~WebContentsImpl() content/browser/web_contents/web_contents_impl.cc:998:14
    #9 0x5580cfa2fd2d in content::WebContentsImpl::~WebContentsImpl() content/browser/web_contents/web_contents_impl.cc:889:37
    #10 0x5580e24f31d4 in operator() buildtools/third_party/libc++/trunk/include/memory:1335:5
    #11 0x5580e24f31d4 in reset buildtools/third_party/libc++/trunk/include/memory:1596:7
    #12 0x5580e24f31d4 in views::WebView::SetWebContents(content::WebContents*) ui/views/controls/webview/webview.cc:93:15
    #13 0x5580e24f2e6b in views::WebView::~WebView() ui/views/controls/webview/webview.cc:70:3
    #14 0x5580e24f370d in views::WebView::~WebView() ui/views/controls/webview/webview.cc:68:21
    #15 0x5580e08e8cd9 in views::View::~View() ui/views/view.cc:237:9
    #16 0x5580e08ea22d in views::View::~View() ui/views/view.cc:210:15
    #17 0x5580e08e8cd9 in views::View::~View() ui/views/view.cc:237:9
    #18 0x5580e08ea22d in views::View::~View() ui/views/view.cc:210:15
    #19 0x5580e08e8cd9 in views::View::~View() ui/views/view.cc:237:9
    #20 0x5580e093ebfd in views::ScrollView::Viewport::~Viewport() ui/views/controls/scroll_view.cc:139:32
    #21 0x5580e08e8cd9 in views::View::~View() ui/views/view.cc:237:9
    #22 0x5580e092fa9d in views::ScrollView::~ScrollView() ui/views/controls/scroll_view.cc:246:25
    #23 0x5580e08e8cd9 in views::View::~View() ui/views/view.cc:237:9
    #24 0x5580e1f4cc55 in ~SheetView chrome/browser/ui/views/payments/payment_request_sheet_controller.cc:59:33
    #25 0x5580e1f4cc55 in payments::(anonymous namespace)::SheetView::~SheetView() chrome/browser/ui/views/payments/payment_request_sheet_controller.cc:59:33
    #26 0x5580e1fa9d47 in operator() buildtools/third_party/libc++/trunk/include/memory:1335:5
    #27 0x5580e1fa9d47 in reset buildtools/third_party/libc++/trunk/include/memory:1596:7
    #28 0x5580e1fa9d47 in ~unique_ptr buildtools/third_party/libc++/trunk/include/memory:1550:19
    #29 0x5580e1fa9d47 in ViewStack::Pop(bool) chrome/browser/ui/views/payments/view_stack.cc:76:5
    #30 0x5580e1eedfa5 in payments::PaymentRequestDialogView::GoBack() chrome/browser/ui/views/payments/payment_request_dialog_view.cc:264:16
    #31 0x5580e1f4c497 in payments::PaymentRequestSheetController::BackButtonPressed()
chrome/browser/ui/views/payments/payment_request_sheet_controller.cc:539:15
    #32 0x5580e07319eb in Run base/callback.h:169:12
    #33 0x5580e07319eb in operator() ui/views/controls/button/button.cc:102:68
    #34 0x5580e07319eb in Invoke<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const base::RepeatingCallback<void ()> &, const ui::Event &>
base/bind_internal.h:379:12
    #35 0x5580e07319eb in MakeItSo<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const base::RepeatingCallback<void ()> &, const ui::Event &>
base/bind_internal.h:637:12
    #36 0x5580e07319eb in RunImpl<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const std::tuple<base::RepeatingCallback<void ()> > &, 0>
base/bind_internal.h:710:12
    #37 0x5580e07319eb in base::internal::Invoker<base::internal::BindState<views::Button::PressedCallback::PressedCallback(base::RepeatingCallback<void ()>)::$_0,
base::RepeatingCallback<void ()> >, void (ui::Event const&)>::Run(base::internal::BindStateBase*, ui::Event const&) base/bind_internal.h:692:12
    #38 0x5580e0735bed in views::ButtonController::OnMouseReleased(ui::MouseEvent const&) ui/views/controls/button/button_controller.cc
    #39 0x5580d9755550 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #40 0x5580e06fa849 in ui::ScopedTargetHandler::OnEvent(ui::Event*) ui/events/scoped_target_handler.cc:28:24
    #41 0x5580d9752dee in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #42 0x5580d9752dee in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #43 0x5580d97525ef in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #44 0x5580d975232a in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #45 0x5580e095b69a in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&) ui/views/widget/root_view.cc:480:9
    #46 0x5580e0979cd0 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc:1318:20
    #47 0x5580d9755550 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #48 0x5580d9752dee in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #49 0x5580d9752dee in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #50 0x5580d97525ef in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #51 0x5580d975232a in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #52 0x5580dbcaf6bd in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #53 0x5580dbccd60f in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:113:16
    #54 0x5580dbccd2b3 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*) ui/events/event_source.cc:138:12
    #55 0x5580e0a38d67 in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*) ui/aura/window_tree_host_platform.cc:246:38
    #56 0x5580e0a33f47 in views::DesktopWindowTreeHostLinux::DispatchEvent(ui::Event*) ui/views/widget/desktop_aura/desktop_window_tree_host_linux.cc:242:29
```

```
    #57 0x5580da7e480d in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event const&) ui/platform_window/x11/x11_window.cc:638:34
    #58 0x5580da7e3b50 in ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc:583:3
    #59 0x5580da7e4a2f in non-virtual thunk to ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc
    #60 0x5580d93c24ab in ui::PlatformEventSource::DispatchEvent(ui::Event*) ui/events/platform/platform_event_source.cc:100:29
    #61 0x5580d98a94a4 in ui::X11EventSource::OnEvent(x11::Event const&) ui/events/platform/x11/x11_event_source.cc:299:5
    #62 0x5580caf49c9c in x11::Connection::DispatchEvent(x11::Event const&) ui/gfx/x/connection.cc:460:14
    #63 0x5580caf48d21 in ProcessNextEvent ui/gfx/x/connection.cc:511:3
    #64 0x5580caf48d21 in x11::Connection::Dispatch() ui/gfx/x/connection.cc:437:5
    #65 0x5580d98a7a45 in ui::X11EventSource::DispatchXEvents() ui/events/platform/x11/x11_event_source.cc:156:25
    #66 0x5580d98b76cb in ui::(anonymous namespace)::XSourceDispatch(_GSource*, int (*)(void*), void*) ui/events/platform/x11/x11_event_watcher_glib.cc:42:15
    #67 0x7f3881cc204d in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x5204d)

0x614000310bb0 is located 368 bytes inside of 392-byte region [0x614000310a40,0x614000310bc8)
freed by thread T0 (chrome) here:
    #0 0x5580c9ae970d 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 0x5580e1ef8cb8 in operator() buildtools/third_party/libc++/trunk/include/memory:1335:5
    #2 0x5580e1ef8cb8 in reset buildtools/third_party/libc++/trunk/include/memory:1596:7
    #3 0x5580e1ef8cb8 in ~unique_ptr buildtools/third_party/libc++/trunk/include/memory:1550:19
    #4 0x5580e1ef8cb8 in ~pair buildtools/third_party/libc++/trunk/include/utility:297:29
    #5 0x5580e1ef8cb8 in destroy<std::pair<views::View *const, std::unique_ptr<payments::PaymentRequestSheetController> >, void, void>
buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:317:15
    #6 0x5580e1ef8cb8 in erase buildtools/third_party/libc++/trunk/include/__tree:2422:5
    #7 0x5580e1ef8cb8 in __erase_unique<views::View *> buildtools/third_party/libc++/trunk/include/__tree:2445:5
    #8 0x5580e1ef8cb8 in erase buildtools/third_party/libc++/trunk/include/map:1306:25
    #9 0x5580e1ef8cb8 in payments::PaymentRequestDialogView::ViewHierarchyChanged(views::ViewHierarchyChangedDetails const&)
chrome/browser/ui/views/payments/payment_request_dialog_view.cc:631:21
    #10 0x5580e09135eb in views::View::ViewHierarchyChangedImpl(views::ViewHierarchyChangedDetails const&) ui/views/view.cc:2641:3
    #11 0x5580e0914b3a in views::View::PropagateRemoveNotifications(views::View*, views::View*, bool) ui/views/view.cc:2596:8
    #12 0x5580e08ebcdd in views::View::DoRemoveChildView(views::View*, bool, bool, views::View*) ui/views/view.cc:2561:9
    #13 0x5580e1fa9d0e in RemoveChildViewT<views::View> ui/views/view.h:447:5
    #14 0x5580e1fa9d0e in ViewStack::Pop(bool) chrome/browser/ui/views/payments/view_stack.cc:76:5
    #15 0x5580e1eedfa5 in payments::PaymentRequestDialogView::GoBack() chrome/browser/ui/views/payments/payment_request_dialog_view.cc:264:16
    #16 0x5580e1f4c497 in payments::PaymentRequestSheetController::BackButtonPressed()
chrome/browser/ui/views/payments/payment_request_sheet_controller.cc:539:15
    #17 0x5580e07319eb in Run base/callback.h:169:12
    #18 0x5580e07319eb in operator() ui/views/controls/button/button.cc:102:68
    #19 0x5580e07319eb in Invoke<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const base::RepeatingCallback<void ()> &, const ui::Event &>
base/bind_internal.h:379:12
    #20 0x5580e07319eb in MakeItSo<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const base::RepeatingCallback<void ()> &, const ui::Event &>
base/bind_internal.h:637:12
    #21 0x5580e07319eb in RunImpl<const (lambda at ../../ui/views/controls/button/button.cc:101:31) &, const std::tuple<base::RepeatingCallback<void ()> > &, 0>
base/bind_internal.h:710:12
    #22 0x5580e07319eb in base::internal::Invoker<base::internal::BindState<views::Button::PressedCallback::PressedCallback(base::RepeatingCallback<void ()>)::$_0,
base::RepeatingCallback<void ()> >, void (ui::Event const&)>::Run(base::internal::BindStateBase*, ui::Event const&) base/bind_internal.h:692:12
    #23 0x5580e0735bed in views::ButtonController::OnMouseReleased(ui::MouseEvent const&) ui/views/controls/button/button_controller.cc
    #24 0x5580d9755550 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #25 0x5580e06fa849 in ui::ScopedTargetHandler::OnEvent(ui::Event*) ui/events/scoped_target_handler.cc:28:24
    #26 0x5580d9752dee in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #27 0x5580d9752dee in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #28 0x5580d97525ef in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #29 0x5580d975232a in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #30 0x5580e095b69a in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&) ui/views/widget/root_view.cc:480:9
    #31 0x5580e0979cd0 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc:1318:20
    #32 0x5580d9755550 in ui::EventHandler::OnEvent(ui::Event*) ui/events/event_handler.cc
    #33 0x5580d9752dee in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #34 0x5580d9752dee in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #35 0x5580d97525ef in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #36 0x5580d975232a in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #37 0x5580dbcaf6bd in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #38 0x5580dbccd60f in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:113:16
    #39 0x5580dbccd2b3 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*) ui/events/event_source.cc:138:12
    #40 0x5580e0a38d67 in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*) ui/aura/window_tree_host_platform.cc:246:38
    #41 0x5580e0a33f47 in views::DesktopWindowTreeHostLinux::DispatchEvent(ui::Event*) ui/views/widget/desktop_aura/desktop_window_tree_host_linux.cc:242:29
    #42 0x5580da7e480d in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event const&) ui/platform_window/x11/x11_window.cc:638:34
    #43 0x5580da7e3b50 in ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc:583:3
    #44 0x5580da7e4a2f in non-virtual thunk to ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc
    #45 0x5580d93c24ab in ui::PlatformEventSource::DispatchEvent(ui::Event*) ui/events/platform/platform_event_source.cc:100:29

previously allocated by thread T0 (chrome) here:
    #0 0x5580c9ae8ead 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 0x5580e1ee8bba in make_unique<payments::PaymentHandlerWebFlowViewController, base::WeakPtr<payments::PaymentRequestSpec>,
base::WeakPtr<payments::PaymentRequestState>, base::WeakPtr<payments::PaymentRequestDialogView>, content::WebContents *, Profile *, const GURL &,
base::OnceCallback<void (bool, int, int)> > buildtools/third_party/libc++/trunk/include/memory:2006:28
    #2 0x5580e1ee8bba in payments::PaymentRequestDialogView::ShowPaymentHandlerScreen(GURL const&, base::OnceCallback<void (bool, int, int)>)
chrome/browser/ui/views/payments/payment_request_dialog_view.cc:169:11
    #3 0x5580d794f8b3 in payments::ChromePaymentRequestDelegate::EmbedPaymentHandlerWindow(GURL const&, base::OnceCallback<void (bool, int, int)>)
chrome/browser/payments/chrome_payment_request_delegate.cc:243:20
    #4 0x5580e27e8ccc in DisplayPaymentHandlerWindow components/payments/content/payment_request_display_manager.cc:42:14
    #5 0x5580e27e8ccc in payments::PaymentRequestDisplayManager::ShowPaymentHandlerWindow(GURL const&, base::OnceCallback<void (bool, int, int)>)
components/payments/content/payment_request_display_manager.cc:65:22
    #6 0x5580d6d3cb32 in ChromeContentBrowserClient::ShowPaymentHandlerWindow(content::BrowserContext*, GURL const&, base::OnceCallback<void (bool, int, int)>)
chrome/browser/chrome_content_browser_client.cc:5304:9
    #7 0x5580cf747521 in content::(anonymous namespace)::ShowPaymentHandlerWindowOnUI(scoped_refptr<content::ServiceWorkerContextWrapper>, GURL const&,
base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>, bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>,
base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>,
std::__1::allocator<char> > > const&)>) content/browser/service_worker/payment_handler_support.cc:83:34
    #8 0x5580cf748719 in void base::internal::FunctorTraits<void (*)(scoped_refptr<content::ServiceWorkerContextWrapper>, GURL const&, base::OnceCallback<void
(base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>,
std::__1::allocator<char> > > const&)>, bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>),
void>::Invoke<void (*)(scoped_refptr<content::ServiceWorkerContextWrapper>, GURL const&, base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>,
bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>),
scoped_refptr<content::ServiceWorkerContextWrapper>, GURL, base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>,
bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)> >
```

(void (*&&)(scoped_refptr<content::ServiceWorkerContextWrapper>, GURL const&, base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>,
bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>),
scoped_refptr<content::ServiceWorkerContextWrapper>&&, GURL&&, base::OnceCallback<void (base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>,
bool, int, int)>&&, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>&&, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>&&)
base/bind_internal.h:393:12
    #9 0x5580ce312238 in Run base/callback.h:101:12
    #10 0x5580ce312238 in content::RunOrPostTaskOnThread(base::Location const&, content::BrowserThread::ID, base::OnceCallback<void ()>)
content/public/browser/browser_thread.cc:20:21
    #11 0x5580cf7470c2 in content::PaymentHandlerSupport::ShowPaymentHandlerWindow(GURL const&, content::ServiceWorkerContextCore*, base::OnceCallback<void
(base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>,
std::__1::allocator<char> > > const&)>, bool, int, int)>, base::OnceCallback<void (base::OnceCallback<void (bool, mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>,
base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)>, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)
content/browser/service_worker/payment_handler_support.cc:103:3
    #12 0x5580cf90d71c in content::ServiceWorkerVersion::OpenPaymentHandlerWindow(GURL const&, base::OnceCallback<void (bool,
mojo::StructPtr<blink::mojom::ServiceWorkerClientInfo>, base::Optional<std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > > const&)>)
content/browser/service_worker/service_worker_version.cc:1423:3
    #13 0x5580cc7875ce in blink::mojom::ServiceWorkerHostStubDispatch::AcceptWithResponder(blink::mojom::ServiceWorkerHost*, mojo::Message*,
std::__1::unique_ptr<mojo::MessageReceiverWithStatus, std::__1::default_delete<mojo::MessageReceiverWithStatus> >)
gen/third_party/blink/public/mojom/service_worker/service_worker.mojom.cc:2221:13
    #14 0x5580d7cbcd76 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*) mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:526:56
    #15 0x5580d7cc8d01 in mojo::MessageDispatcher::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/message_dispatcher.cc:43:19
    #16 0x5580d7cd4516 in mojo::internal::MultiplexRouter::ProcessIncomingMessage(mojo::internal::MultiplexRouter::MessageWrapper*,
mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*) mojo/public/cpp/bindings/lib/multiplex_router.cc:955:42
    #17 0x5580d7cd2c08 in mojo::internal::MultiplexRouter::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/multiplex_router.cc:622:38
    #18 0x5580d7cc8d01 in mojo::MessageDispatcher::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/message_dispatcher.cc:43:19
    #19 0x5580d7cb65c4 in mojo::Connector::DispatchMessage(mojo::Message) mojo/public/cpp/bindings/lib/connector.cc:508:49
    #20 0x5580d7cb7fa0 in mojo::Connector::ReadAllAvailableMessages() mojo/public/cpp/bindings/lib/connector.cc:566:14
    #21 0x5580d7d1e68d in Run base/callback.h:169:12
    #22 0x5580d7d1e68d in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&) mojo/public/cpp/system/simple_watcher.cc:278:14
    #23 0x5580d7d1f854 in Invoke<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &), base::WeakPtr<mojo::SimpleWatcher>, int, unsigned
int, mojo::HandleSignalsState> base/bind_internal.h:498:12
    #24 0x5580d7d1f854 in MakeItSo<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &), base::WeakPtr<mojo::SimpleWatcher>, int,
unsigned int, mojo::HandleSignalsState> base/bind_internal.h:657:5
    #25 0x5580d7d1f854 in RunImpl<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &), std::tuple<base::WeakPtr<mojo::SimpleWatcher>,
int, unsigned int, mojo::HandleSignalsState>, 0, 1, 2, 3> base/bind_internal.h:710:12
    #26 0x5580d7d1f854 in base::internal::Invoker<base::internal::BindState<void (mojo::SimpleWatcher::*)(int, unsigned int, mojo::HandleSignalsState const&),
base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:679:12
    #27 0x5580d62f6c56 in Run base/callback.h:101:12
    #28 0x5580d62f6c56 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:168:33
    #29 0x5580d6332477 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #30 0x5580d6331ca4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #31 0x5580d61f4809 in HandleDispatch base/message_loop/message_pump_glib.cc:374:46
    #32 0x5580d61f4809 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) base/message_loop/message_pump_glib.cc:124:43
    #33 0x7f3881cc217c in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x5217c)

SUMMARY: AddressSanitizer: heap-use-after-free components/web_modal/web_contents_modal_dialog_manager.cc:116:16 in BlockWebContentsInteraction
Shadow bytes around the buggy address:
  0x0c288005a120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c288005a130: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c288005a140: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c288005a150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c288005a160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c288005a170: fd fd fd fd fd fd[fd]fd fd fa fa fa fa fa fa fa
  0x0c288005a180: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c288005a190: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c288005a1a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c288005a1b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c288005a1c0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==137616==ABORTING
hide4@hide4-virtual-machine:~/fuzzBrowser/chromium_version/asan-linux-release-861920$

Comment 11 by maxlg@chromium.org on Wed, Mar 31, 2021, 11:21 PM EDT

0xasnine, is it reproducible on other official versions on your side?

Comment 12 by 0xasn...@gmail.com on Wed, Mar 31, 2021, 11:34 PM EDT

Hi, I also can't reproduce it in the official Chrome Canary  or Chrome dev versions.

Comment 13 by maxlg@chromium.org on Wed, Mar 31, 2021, 11:48 PM EDT

**Status:** Available (was: Assigned)
**Owner:** ----
**Cc:** maxlg@chromium.org
**Labels:** Web-Payments-ZBB Pri-3

#c12, thanks for your confirmation. I will lower the priority since it's not found to happen in official version yet. Having said that, there could be other ways to trigger it so it could still be an issue.

Comment 14 by maxlg@chromium.org on Wed, Mar 31, 2021, 11:48 PM EDT

Description was changed.

Comment 15 by maxlg@chromium.org on Thu, Apr 1, 2021, 10:35 AM EDT

"heap-use-after-free in the payment dialog in the browser process which will excape the sandbox."

Security team: I don't understand why it is a security bug. Isn't it just a crash?

Comment 16 by sheriffbot on Thu, Apr 1, 2021, 1:02 PM EDT

**Labels:** M-90 Target-90

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

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

Comment 17 by sheriffbot on Thu, Apr 1, 2021, 1:38 PM EDT

**Labels:** -Pri-3 Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 18 by adetaylor@google.com on Tue, Apr 6, 2021, 1:43 PM EDT

maxlg@ re #c15 use-after-frees can readily be exploited by attackers to achieve arbitrary code execution. Attackers use the same underlying bug to corrupt memory in precise and deliberate ways rather than in a way which crashes. They have to carefully arrange other objects on the heap such that they control the data which is read during the UaF. This is fiddly, but attackers have versatile toolkits to make such things as reliable as possible.

As this is the browser process, that would give a remote attacker full access to the device and all cross-origin data. As such browser process use-after-frees are usually Critical severity and priority 0, usually necessitating an emergency refresh of Chrome pushed to all our users within a few days. In this case, its severity is mitigated down to Medium by the need to install payment methods and interact with the UI.

Comment 19 by maxlg@chromium.org on Tue, Apr 6, 2021, 1:58 PM EDT

Does it affect the security severity now that it's not reproducible on official releases (only reproducible on asan releases)?

Comment 20 by cthomp@chromium.org on Tue, Apr 6, 2021, 6:22 PM EDT

**Owner:** maxlg@chromium.org

Security sheriff here: Assigning this back to maxlg@. We try to keep all security bugs assigned to owners so that there is someone responsible for moving them toward resolution.

As for severity, it's possible that this isn't reachable in normal released builds, but something triggering in ASAN typically just means its _easier_ to trigger there (in that ASAN causes it to be a crash instead of silent memory corruption). Unlike for features that are disabled in release builds (e.g., features behind the Experimental Web Platform Features flag), we don't downgrade the Security_Impact of bugs that only repro in ASAN.

Comment 21 by maxlg@chromium.org on Tue, Apr 6, 2021, 11:11 PM EDT

**Status:** Assigned (was: Available)

It seems like payment_handler_web_flow_view_controller's dialog_manager_delegate_ is released elsewhere before being used in web_contents_modal_dialog_manager. It's not obvious to me how it is possible to happen.

Comment 22 by 0xasn...@gmail.com on Sun, Apr 18, 2021, 11:51 PM EDT

Hi, it seems that this issue affects the latest Version 92.0.4479.3 (Official Build) canary (64-bit) ~

Comment 23 by 0xasn...@gmail.com on Mon, Apr 19, 2021, 12:01 AM EDT

The prowser process crash log:

```
(2cc0.2ff4): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
chrome_7ffd672c0000!ovly_debug_event+0x1ea219b:
00007ffd`6d510ffb 488b00          mov     rax,qword ptr [rax] ds:efefefef`efefefef=????????????????
0:000> kv
 # Child-SP          RetAddr               : Args to Child                                                   : Call Site
00 000000f0`819fd070 00007ffd`681efad0     : 00000318`00c9ed00 00007ffd`6a085c3f 00007ffd`6faabd70 00007ffd`68688e04 :
chrome_7ffd672c0000!ovly_debug_event+0x1ea219b
01 000000f0`819fd0b0 00007ffd`6a17e3b9     : aaaaaaaa`aaaaaaaa 00007ffd`69d19dc0 00007ffd`69d19dc0 00000318`01305440 :
chrome_7ffd672c0000!ChromeMain+0x866d40
02 000000f0`819fd160 00007ffd`6b2e9378     : ffffffff`ffffffff 000073e6`02cb4fe7 00000000`00000000 00000000`00000000 :
chrome_7ffd672c0000!GetHandleVerifier+0x10bd3c9
03 000000f0`819fd190 00007ffd`6887f950     : 000073e6`02cb4d07 00000000`00000000 00000000`00000000 000073e6`02cb4d57 :
chrome_7ffd672c0000!GetHandleVerifier+0x2228388
04 000000f0`819fd2c0 00007ffd`683ebb94     : 00000000`00000000 00000318`00d10480 00000318`00d10480 00000318`0130aa08 :
chrome_7ffd672c0000!RelaunchChromeBrowserWithNewCommandLineIfNeeded+0x4a5130
05 000000f0`819fd370 00007ffd`683d1d46     : 000073e6`02cb4b57 00000318`011cd008 00000318`0074d430 00000000`00000001 :
chrome_7ffd672c0000!RelaunchChromeBrowserWithNewCommandLineIfNeeded+0x11374
06 000000f0`819fd450 00007ffd`683d1c70     : 000073e6`02cb4b27 00007ffd`672c1262 00000318`0074d430 00000318`02135100 :
chrome_7ffd672c0000!ChromeMain+0xa48fb6
07 000000f0`819fd4a0 00007ffd`677b3f57     : 000000f0`819fdd10 00007ffd`6a085c3f 000073e6`02cb4bf7 00007ffd`6a085c3f :
chrome_7ffd672c0000!ChromeMain+0xa48ee0
08 000000f0`819fd4e0 00007ffd`680fca30     : 00000318`0074d430 00000000`00000001 00000318`00bef9c0 000000f0`00000000 :
chrome_7ffd672c0000!IsSandboxedProcess+0x437fb7
09 000000f0`819fd590 00007ffd`677b3f57     : 000000f0`819fdd10 00007ffd`6a085c3f 000073e6`02cb4ae7 00007ffd`6a085c3f :
chrome_7ffd672c0000!ChromeMain+0x773ca0
0a 000000f0`819fd5d0 00007ffd`680fca30     : 00000318`022f4010 00007ffd`677b43d1 00000318`022f40a8 00000318`022f4068 :
chrome_7ffd672c0000!IsSandboxedProcess+0x437fb7
0b 000000f0`819fd680 00007ffd`677b3f57     : 00000318`022017a0 00000318`022017a0 00007ffd`712ab408 00007ffd`6a085c3f :
chrome_7ffd672c0000!ChromeMain+0x773ca0
0c 000000f0`819fd6c0 00007ffd`6d5b24b0     : 00000000`00000000 00000000`00000000 00000000`00000000 00007ffd`672c1262 :
chrome_7ffd672c0000!IsSandboxedProcess+0x437fb7
0d 000000f0`819fd770 00007ffd`677b3f57     : 00000318`02105280 000000f0`00000000 00000318`004ddd00 000000f0`819fda60 :
chrome_7ffd672c0000!ovly_debug_event+0x1f43650
0e 000000f0`819fd7b0 00007ffd`6d5b2150     : 00000318`0074d430 00000000`00000001 00000318`01136e00 000000f0`00000000 :
chrome_7ffd672c0000!IsSandboxedProcess+0x437fb7
0f 000000f0`819fd860 00007ffd`677b3f57     : 00000318`009e1e80 00000318`00d01608 00000318`01136e00 00007ffd`680fc713 :
chrome_7ffd672c0000!ovly_debug_event+0x1f432f0
10 000000f0`819fd8a0 00007ffd`69816a4b     : 000000f0`819fdd10 00007ffd`68ef6638 000073e6`02cb4667 00000000`012ba700 :
chrome_7ffd672c0000!IsSandboxedProcess+0x437fb7
11 000000f0`819fd950 00007ffd`6f07e4ef     : 00000000`00000000 00000000`00000000 000073e6`02cb4777 00000318`00c70440 :
chrome_7ffd672c0000!GetHandleVerifier+0x755a5b
12 000000f0`819fd990 00007ffd`6f07e3e1     : 000000f0`819fdd10 00007ffd`6f07d33d 000073e6`02cb4697 00007ffd`6febce60 :
```

chrome_7ffd672c0000!ovly_debug_event+0x3a0f68f
13 000000f0`819fda00 00007ffd`6f2c99f3 : 000073e6`02cb4557 00000000`00000002 00000318`0074d430 00000318`0114e6ec :
chrome_7ffd672c0000!ovly_debug_event+0x3a0f581
14 000000f0`819fda40 00007ffd`6d0c877b : 00000018`00000018 00007ffd`6d5abfe3 00000318`0114e300 00000318`021e3de0 :
chrome_7ffd672c0000!ovly_debug_event+0x3c5ab93
15 000000f0`819fdaa0 00007ffd`6d5abd00 : 3f800000`00000000 00000000`00000000 80000000`80000000 80000000`80000000 :
chrome_7ffd672c0000!ovly_debug_event+0x1a5991b
16 000000f0`819fdae0 00007ffd`6b3165f5 : 00000000`00000008 00000000`00000008 00000000`00000008 00007ffd`6a08486f :
chrome_7ffd672c0000!ovly_debug_event+0x1f3cea0
17 000000f0`819fdb40 00007ffd`6e45715f : 00000318`02122020 00000318`02122030 00000318`02122030 00007ffd`6a1a551a :
chrome_7ffd672c0000!GetHandleVerifier+0x2255605
18 000000f0`819fdcf0 00007ffd`67c0312e : 000073e6`02cb4397 00000318`0114e300 aaaaaaaa`aaaaaaaa aaaaaaaa`aaaaaaaa :
chrome_7ffd672c0000!ovly_debug_event+0x2de82ff
19 000000f0`819fdd60 00007ffd`6d5b605a : 00000000`00000000 00000000`7fc00000 000000f0`819fde58 00000002`00000030 :
chrome_7ffd672c0000!ChromeMain+0x27a39e
1a 000000f0`819fde10 00007ffd`68efb0c5 : 000001dd`000007a8 000073e6`02cb4007 000000f0`819fdfd0 00007ffd`6ff00810 :
chrome_7ffd672c0000!ovly_debug_event+0x1f471fa
1b 000000f0`819fdf70 00007ffd`6b3165f5 : 00000318`0127d570 00000000`00000040 00000000`00000040 00000000`00000005 :
chrome_7ffd672c0000!RelaunchChromeBrowserWithNewCommandLineIfNeeded+0xb208a5
1c 000000f0`819fe040 00007ffd`67c0312e : 00000000`aaaaaa02 000073e6`02cb7fe7 aaaaaaaa`aaaaaaaa aaaaaaaa`aaaaaaaa :
chrome_7ffd672c0000!GetHandleVerifier+0x2255605
1d 000000f0`819fe1f0 00007ffd`67c02c70 : 0fffffff`ffffffff 00007ffd`6b5d7367 000000f0`819fe2e8 00007ffd`67755911 : chrome_7ffd672c0000!ChromeMain+0x27a39e
1e 000000f0`819fe2a0 00007ffd`67f9e434 : 00000000`00000202 000000f0`819fe570 00000000`00000004 00000318`003b5280 :
chrome_7ffd672c0000!ChromeMain+0x279ee0
1f 000000f0`819fe330 00007ffd`69256377 : 000000f0`819fe558 00007ffd`67f8f1b3 00000318`00d9bc30 00007ffd`67f8f0b1 :
chrome_7ffd672c0000!ChromeMain+0x6156a4
20 000000f0`819fe3c0 00007ffd`67f8eae0 : 00000000`00000020 00007ffd`fefa67ac 000000f0`819fe5d0 000000f0`819fe510 :
chrome_7ffd672c0000!GetHandleVerifier+0x195387
21 000000f0`819fe410 00007ffd`67f7ce40 : 00000000`00000000 00000000`00070000 000001f6`b0bd1b70 00000000`00000202 :
chrome_7ffd672c0000!ChromeMain+0x605d50
22 000000f0`819fe700 00007ffd`67f7afa8 : 00000000`00000001 00007ffd`6aaa7f4c 00000000`00000000 00007ffd`6aaf95b8 :
chrome_7ffd672c0000!ChromeMain+0x5f40b0
23 000000f0`819fe8b0 00007ffd`6775bdad : 00000000`00000000 00000000`00000000 0000000b`1ab01d39 aaaaaaaa`aaaaaaaa :
chrome_7ffd672c0000!ChromeMain+0x5f2218
24 000000f0`819fe9c0 00007ffd`6775bd1f : 00000000`00000000 00000000`00100e60 0000972c`3e133b15 00000000`00000000 :
chrome_7ffd672c0000!IsSandboxedProcess+0x3dfe0d
25 000000f0`819fea30 00007ffd`fe5fe858 : 00000000`00100e60 00000000`00000000 00000000`00000001 00000000`00000001 :
chrome_7ffd672c0000!IsSandboxedProcess+0x3dfd7f
26 000000f0`819fea60 00007ffd`fe5fe299 : 000000f0`819fee10 00007ffd`6775bd10 00000000`00150b90 00007ffd`00000202 : user32!UserCallWinProcCheckWow+0x2f8
27 000000f0`819febf0 00007ffd`674ceab4 : 00007ffd`6775bd10 00000318`002e4240 00000318`00d98d18 00000000`00000000 :
user32!DispatchMessageWorker+0x249
28 000000f0`819fec70 00007ffd`6aeaee22 : 00000000`00000000 00000318`002cc488 00000318`002e4240 00000000`0000002d :
chrome_7ffd672c0000!IsSandboxedProcess+0x152b14
29 000000f0`819feda0 00007ffd`6a084352 : 00000000`00000008 00007ffd`6aaa7f4c 00000318`010aa570 00007ffd`67fd8a74 :
chrome_7ffd672c0000!GetHandleVerifier+0x1dede32
2a 000000f0`819fef10 00007ffd`67c60789 : 00000318`010aa570 00007ffd`686ef689 00000318`00d98f08 00007ffd`6a9890d6 :
chrome_7ffd672c0000!GetHandleVerifier+0xfc3362
2b 000000f0`819fef70 00007ffd`67eb7810 : 00aaaaaa`aaaaaaaa 00000318`00417e00 00000000`0000002d 80000000`00000030 :
chrome_7ffd672c0000!ChromeMain+0x2d79f9
2c 000000f0`819fefd0 00007ffd`683dccbf : 00000000`00000030 000000f0`819ff1b8 0000000b`18d2ced9 00000000`000b9ce2 :
chrome_7ffd672c0000!ChromeMain+0x52ea80
2d 000000f0`819ff120 00007ffd`69e12b23 : aaaaaaaa`aaaaaaaa 000000f0`819ff300 00000000`00000000 00000318`0006c140 :
chrome_7ffd672c0000!RelaunchChromeBrowserWithNewCommandLineIfNeeded+0x249f
2e 000000f0`819ff190 00007ffd`6a0778ac : 00000318`0007c480 00007ffd`6af61862 aaaaaaaa`aaaaaaaa 00007ffd`6ada1c7f :
chrome_7ffd672c0000!GetHandleVerifier+0xd51b33
2f 000000f0`819ff230 00007ffd`6798b19f : 00000318`0007c2c0 000000f0`819ff4a8 00000000`00002ff4 80000000`00000000 :
chrome_7ffd672c0000!GetHandleVerifier+0xfb68bc
30 000000f0`819ff380 00007ffd`67988f1f : 00000318`0007c2c0 00007ff6`b13c0000 000000f0`819ff700 00000000`00000000 :
chrome_7ffd672c0000!ChromeMain+0x240f
31 000000f0`819ff590 00007ff6`b146e1ee : 00000000`00000201 00007ffd`67988d90 00000000`00000000 000000f0`819ff710 :
chrome_7ffd672c0000!ChromeMain+0x18f
32 000000f0`819ff6a0 00007ff6`b146dda7 : 00000000`0000000a 00000000`00000000 000000f0`819ffa90 00007ffd`feee2228 : chrome!GetHandleVerifier+0x5887e
33 000000f0`819ff910 00007ff6`b14d16c2 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : chrome!GetHandleVerifier+0x58437
34 000000f0`819ffd10 00007ffd`fe8d7034 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : chrome!IsSandboxedProcess+0x5f6c2
35 000000f0`819ffd50 00007ffd`fef02651 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 :
KERNEL32!BaseThreadInitThunk+0x14
36 000000f0`819ffd80 00000000`00000000 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21

Comment 24 by maxlg@chromium.org on Mon, Apr 19, 2021, 12:38 AM EDT

Thanks for the update! Which platform was it on? Could you send me the crash ID of the crash on chrome://crashes/? Thanks!

I've just tested it on Mac with 92.0.4481.0, not reproducible.

Comment 25 by 0xasn...@gmail.com on Mon, Apr 19, 2021, 1:52 AM EDT

I test it on Windows and I have closed the crash update.
I update the canary version to 92.0.4482.0 and couldn't reproduce it either~

Comment 26 by 0xasn...@gmail.com on Mon, Apr 19, 2021, 2:02 AM EDT

Crash from Monday, April 19, 2021 at 11:58:16 AM
Status: Uploaded
Uploaded Crash Report ID: 3be17628b9841383
Upload Time: Monday, April 19, 2021 at 2:01:30 PM

Comment 27 by 0xasn...@gmail.com on Mon, Apr 19, 2021, 2:09 AM EDT

It can also been reproduced the UAF in chromium-browser-asan/win32-release_x64/asan-win32-release_x64-873690.zip on Windows.

Comment 28 by maxlg@chromium.org on Mon, Apr 19, 2021, 3:32 PM EDT

**Cc:** rouslan@chromium.org smcgruer@chromium.org nburris@chromium.org

+folks for visibility

Comment 29 by rouslan@chromium.org on Mon, Apr 19, 2021, 4:02 PM EDT

Nick: This appears related to dialogs on top of the payment handler window. You've recently fixed this issue in M-92 and M-91 with https://chromiumdash.appspot.com/commit/2a762314d99e45c4879ee77d41166cbcb167a21c. Do you know if this issue could be fixed by your patch as well?

Comment 30 by rouslan@chromium.org on Mon, Apr 19, 2021, 5:15 PM EDT

Max: Are you able to reproduce based on the steps and the attachments?

Comment 31 by nburris@google.com on Mon, Apr 19, 2021, 5:21 PM EDT

Re #c29, that fix (for a different bug) is in canary 92.0.4479.0, and I can't reproduce this crash myself, but #c22 reproduced on 92.0.4479.3 so it's unlikely that fixed this bug as well. The crash steps also don't involve multiple browser windows so my patch should be unrelated.

Based on the recordings and stack traces the issue looks to be when PaymentHandlerWebFlowViewController navigates to an external URL (which should probably just be aborted?)

Comment 32 by rouslan@chromium.org on Mon, Apr 19, 2021, 5:25 PM EDT

> ... navigates to an external URL (which should probably just be aborted?)

One of the external URLs is http://localhost, which we allow for testing purposes. The other external URL is skype:asdf, but navigation is blocked by a dialog before we have a chance to abort anything.

Comment 33 Deleted

Comment 34 by maxlg@chromium.org on Mon, Apr 19, 2021, 5:39 PM EDT

I am not able to reproduce it with a 92.0.4483.0 local build.

Comment 35 by rouslan@chromium.org on Mon, Apr 19, 2021, 5:39 PM EDT

Which part of the repro fails for you, Max?

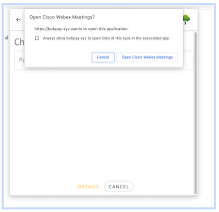
Comment 36 by maxlg@chromium.org on Mon, Apr 19, 2021, 5:56 PM EDT

By not able to reproduce I meant nothing crashed on my side.

Comment 37 by rouslan@chromium.org on Mon, Apr 19, 2021, 6:05 PM EDT

The vanilla (non-asan) build of Chrome Canary does not crash when I type in window.location.href="wbx://servername" in the developer tools console window. So this may be easier to detect in an ASAN build.

**Screen Shot 2021-04-19 at 6.02.45 PM.png**
75.0 KB View Download




Comment 38 by maxlg@chromium.org on Mon, Apr 19, 2021, 6:39 PM EDT

#c34, sorry my bad.. the crash is reproducible with 92.0.4483.0 local build.

Comment 39 by rouslan@chromium.org on Mon, Apr 19, 2021, 6:43 PM EDT

That's great news! Does that make a fix easier to figure out?

Comment 40 by maxlg@chromium.org on Mon, Apr 19, 2021, 6:46 PM EDT

Easier steps to reproduce:
* Open https://liquangumax.github.io/lindapay/, install
* Open https://liquangumax.github.io/lindapay2/, install
* Open https://maxlgu.github.io/pr/lindapay-github/, buy
* Click "continue"
* Click the link "Directory Picker"
* Click "Open the file dir", click "select"
* Click the back button, boom

Comment 41 by maxlg@chromium.org on Mon, Apr 19, 2021, 6:50 PM EDT

Description was changed.

Comment 42 by maxlg@chromium.org on Mon, Apr 19, 2021, 7:13 PM EDT

Description was changed.

Comment 43 by maxlg@chromium.org on Mon, Apr 19, 2021, 7:15 PM EDT

Description was changed.

Comment 44 by maxlg@chromium.org on Mon, Apr 19, 2021, 8:38 PM EDT

GoBack() is entered only once during the crash.

It was reproducible on 87.0.4258.0, so CL[1] was not the culprit.

[1] https://chromium-review.googlesource.com/c/chromium/src/+/2391900

Comment 45 by maxlg@chromium.org on Mon, Apr 19, 2021, 8:40 PM EDT

Description was changed.

Comment 46 by maxlg@chromium.org on Mon, Apr 19, 2021, 8:52 PM EDT

**Cc:** a...@chromium.org

CC avi@, are you familiar with web_contents_modal_dialog_manager.cc? This crash is related to the class.

Comment 47 by a...@chromium.org on Mon, Apr 19, 2021, 9:18 PM EDT

**Cc:** robliao@chromium.org

I'm not familiar with its implementation. Rob, do you have knowledge here?

Comment 48 by robliao@chromium.org on Tue, Apr 20, 2021, 8:28 PM EDT

**Owner:** wittman@chromium.org

Routing to wittman@ for WebContentsModalDialogManager

Comment 49 by wittman@chromium.org on Tue, Apr 20, 2021, 9:09 PM EDT

**Owner:** maxlg@chromium.org
**Cc:** wittman@chromium.org

I believe the description in #c21 is correct, and that the appropriate fix is for PaymentHandlerWebFlowViewController to unset the dialog_manager_delegate_ on the WebContentsModalDialogManager before the delegate is destroyed.

See an example of doing this for another dialog at
https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ash/login/ui/webui_login_view.cc;drc=3eb027037d29138f58f98356af0295fc17030f0e;l=142

Comment 50 by maxlg@chromium.org on Wed, Apr 21, 2021, 3:00 PM EDT

Thanks for the advise. The fix works!

WIP CL: https://chromium-review.googlesource.com/c/chromium/src/+/2844509

Comment 51 by rouslan@chromium.org on Wed, Apr 21, 2021, 3:59 PM EDT

Max, is this the only dialog where we need to unset the `dialog_manager_delegate_`? Do we have other dialogs that need to do the same thing? For example, what about the SPC dialogs that we've recently built?

Comment 52 by maxlg@chromium.org on Thu, Apr 22, 2021, 4:24 PM EDT

#c51, I don't know. Need to check.

Comment 53 by maxlg@chromium.org on Thu, Apr 22, 2021, 11:44 PM EDT

#c51, this is the only payment code that uses WebContentsModalDialogManager::SetDelegate(). SPC doesn't use WebContentsModalDialogManager.

Comment 54 by rouslan@chromium.org on Fri, Apr 23, 2021, 11:15 AM EDT

Great to hear! Thank you for checking. I look forward to the fix 😀.

Comment 55 by Git Watcher on Fri, Apr 23, 2021, 5:54 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/8f6ad3de87d3d7b375f75004b1389604887d31fb

commit 8f6ad3de87d3d7b375f75004b1389604887d31fb
Author: Liquan (Max) Gu <maxlg@chromium.org>
Date: Fri Apr 23 21:53:25 2021

Clean up WebContentsModalDialogManagerDelegate in desktop Payment UI

payment_request_dialog_view's controller_map_ store the
PaymentHandlerWebFlowViewController and its web-view as a key-value
pair. When the view is popped from payment_request_dialog_view's view
stack, the key-pair will be destroyed. If the controller doesn't reset
WebContentsModalDialogManager's delegate in the controller's destructor,
the WebView's destructor will attempt to access into
WebContentsModalDialogManager's delegate, and cause a use-after-free
crash.

This CL fixes this issue by making sure
PaymentHandlerWebFlowViewController's destructor resets
WebContentsModalDialogManager's delegate.

~~Bug: 1194058~~
Change-Id: Iead54db4b3e682bbccccddf335780c5ceff2e990
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2844509
Commit-Queue: Liquan (Max) Gu <maxlg@chromium.org>
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Commit-Position: refs/heads/master@{#875868}

[modify] https://crrev.com/8f6ad3de87d3d7b375f75004b1389604887d31fb/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 56 by maxlg@chromium.org on Fri, Apr 23, 2021, 5:57 PM EDT

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

Comment 57 by sheriffbot on Sat, Apr 24, 2021, 12:41 PM EDT

**Labels:** reward-topanel

Comment 58 by sheriffbot on Sat, Apr 24, 2021, 2:01 PM EDT

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

Comment 59 by sheriffbot on Sat, Apr 24, 2021, 2:26 PM EDT

**Labels:** Merge-Request-91

Requesting merge to beta M91 because latest trunk commit (875868) appears to be after beta branch point (870763).

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

Comment 60 by sheriffbot on Sat, Apr 24, 2021, 5:57 PM EDT

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

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review
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 61 by pbommana@google.com on Mon, Apr 26, 2021, 12:27 AM EDT

**Cc:** adetaylor@chromium.org pbomm...@chromium.org

maxlg@ please reply to questions posted in comment#60. thank you.

+Adetaylor(Security TPM)

Comment 62 by maxlg@chromium.org on Mon, Apr 26, 2021, 10:32 AM EDT

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
Yes

2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2844509

3. Has the change landed and been verified on ToT?
Yes

4. Does this change need to be merged into other active release branches (M-1, M+1)?
M91, M90

5. Why are these changes required in this milestone after branch?
This is a use-after-free bug which can readily be exploited by attackers to achieve arbitrary code execution. As this is the browser process, that would give a remote attacker full access to the device and all cross-origin data. As such browser process use-after-frees are usually Critical severity and priority 0, usually necessitating an emergency refresh of Chrome pushed to all our users within a few days. In this case, its severity is mitigated down to Medium by the need to install payment methods and interact with the UI.

(Read #c18 for context)

6. Is this a new feature?
No

7. If it is a new feature, is it behind a flag using finch?
No

Comment 63 by maxlg@chromium.org on Mon, Apr 26, 2021, 11:11 AM EDT

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

Changed back to started for visibility.

Comment 64 by maxlg@chromium.org on Mon, Apr 26, 2021, 11:45 AM EDT

Adetaylor, please evaluate whether merging to M90 is required given (5).

Comment 65 by maxlg@chromium.org on Mon, Apr 26, 2021, 12:18 PM EDT

Description was changed.

Comment 66 by adetaylor@chromium.org on Mon, Apr 26, 2021, 2:59 PM EDT

**Labels:** -Merge-Review-91 Merge-Approved-91

maxlg@ do you consider this fully fixed? If so please mark it as such - https://chromium.googlesource.com/chromium/src/+/master/docs/security/security-labels.md#TOC-Merge-labels

Approving merge to M91, branch 4472, assuming no problems have shown up in Canary.

I'm a little surprised Sheriffbot didn't ask to merge this to M90 as well. I'll take an action to work out why.

Comment 67 by maxlg@chromium.org on Mon, Apr 26, 2021, 3:32 PM EDT

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

#c66, thanks for the pointer. Yes, this is fully fixed.

Comment 68 by Git Watcher on Mon, Apr 26, 2021, 4:21 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/08dbfa33cb45c3cfd0891a0c547c861060a110ac

commit 08dbfa33cb45c3cfd0891a0c547c861060a110ac
Author: Liquan (Max) Gu <maxlg@chromium.org>
Date: Mon Apr 26 20:20:20 2021

[M91]Clean up WebContentsModalDialogManagerDelegate in desktop Payment UI

payment_request_dialog_view's controller_map_ store the
PaymentHandlerWebFlowViewController and its web-view as a key-value
pair. When the view is popped from payment_request_dialog_view's view
stack, the key-pair will be destroyed. If the controller doesn't reset
WebContentsModalDialogManager's delegate in the controller's destructor,
the WebView's destructor will attempt to access into
WebContentsModalDialogManager's delegate, and cause a use-after-free
crash.

This CL fixes this issue by making sure
PaymentHandlerWebFlowViewController's destructor resets
WebContentsModalDialogManager's delegate.

(cherry picked from commit 8f6ad3de87d3d7b375f75004b1389604887d31fb)

~~Bug: 1194059~~
Change-Id: Iead54db4b3e682bbccccddf335780c5ceff2e990
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2844509
Commit-Queue: Liquan (Max) Gu <maxlg@chromium.org>
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875868}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2845001
Cr-Commit-Position: refs/branch-heads/4472@{#425}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/08dbfa33cb45c3cfd0891a0c547c861060a110ac/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 69 by maxlg@chromium.org on Mon, Apr 26, 2021, 4:24 PM EDT

**Labels:** Merge-Request-90

Comment 70 by maxlg@chromium.org on Tue, Apr 27, 2021, 10:35 AM EDT

Ping adetaylor@, can I get approved to merge into M90?

Comment 71 by adetaylor@chromium.org on Tue, Apr 27, 2021, 1:01 PM EDT

In general we would only approve merges to the current stable branch a few days before we make the next release, to give maximal bake time for problems to show up in Canary/beta/etc. That's probably about a week away.

Comment 72 by amyressler@google.com on Wed, Apr 28, 2021, 7:24 PM EDT

**Labels:** -reward-topanel reward-unpaid reward-15000

*** 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 73 by amyressler@chromium.org on Wed, Apr 28, 2021, 7:47 PM EDT

Congratulations! The VRP Panel has decided to award you $15000 for this report. Excellent work!

Comment 74 by amyressler@google.com on Fri, Apr 30, 2021, 1:54 PM EDT

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

Comment 75 by adetaylor@google.com on Tue, May 4, 2021, 12:58 PM EDT

**Labels:** -Merge-Request-90 Merge-Approved-90

Approving merge to M90, branch 4430. Please merge by EOD PST Thursday for inclusion in next week's security refresh.

Comment 76 by maxlg@chromium.org on Tue, May 4, 2021, 12:59 PM EDT

Submitting - https://chromium-review.googlesource.com/c/chromium/src/+/2849774.

Comment 77 by Git Watcher on Tue, May 4, 2021, 2:33 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3e2beb764726f0e0a151af76910e189bafbaa97d

commit 3e2beb764726f0e0a151af76910e189bafbaa97d
Author: Liquan (Max) Gu <maxlg@chromium.org>
Date: Tue May 04 18:32:52 2021

[M90]Clean up WebContentsModalDialogManagerDelegate in desktop Payment UI

payment_request_dialog_view's controller_map_ store the
PaymentHandlerWebFlowViewController and its web-view as a key-value
pair. When the view is popped from payment_request_dialog_view's view
stack, the key-pair will be destroyed. If the controller doesn't reset
WebContentsModalDialogManager's delegate in the controller's destructor,
the WebView's destructor will attempt to access into
WebContentsModalDialogManager's delegate, and cause a use-after-free
crash.

This CL fixes this issue by making sure
PaymentHandlerWebFlowViewController's destructor resets
WebContentsModalDialogManager's delegate.

(cherry picked from commit 8f6ad3de87d3d7b375f75004b1389604887d31fb)

~~Bug: 1194958~~
Change-Id: Iead54db4b3e682bbccccddf335780c5ceff2e990
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2844509
Commit-Queue: Liquan (Max) Gu <maxlg@chromium.org>
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875868}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2849774
Cr-Commit-Position: refs/branch-heads/4430@{#1388}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/3e2beb764726f0e0a151af76910e189bafbaa97d/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 78 by amyressler@chromium.org on Fri, May 7, 2021, 5:33 PM EDT

**Labels:** Release-3-M90

Comment 79 by vsavu@google.com on Mon, May 10, 2021, 9:16 AM EDT

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

Comment 80 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT

**Labels:** CVE-2021-30519 CVE_description-missing

Comment 81 by maxlg@chromium.org on Mon, May 10, 2021, 10:04 AM EDT

I believe that we don't need to merge to M86. The users who had older M86 will get upgraded to the current stable version (M90). Is there any way that users can benefit from a new M86?

Comment 82 by rouslan@google.com on Mon, May 10, 2021, 11:22 AM EDT

Chrome OS long-term-support (LTS) users of M86 will benefit. Usually the Chrome OS team takes care of the merge, so no action is needed from our side, Max.

Comment 83 by maxlg@chromium.org on Mon, May 10, 2021, 11:35 AM EDT

Thanks for the explanation! For future reference, vsavu@ also gave me some context: go/4240-merge.

Comment 84 by Git Watcher on Wed, May 12, 2021, 4:54 AM EDT

**Labels:** merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a5c6b0255c70aec702bf9952117063549679cf29

commit a5c6b0255c70aec702bf9952117063549679cf29
Author: Liquan (Max) Gu <maxlg@chromium.org>
Date: Wed May 12 08:52:12 2021

[M90]Clean up WebContentsModalDialogManagerDelegate in desktop Payment UI

payment_request_dialog_view's controller_map_ store the
PaymentHandlerWebFlowViewController and its web-view as a key-value
pair. When the view is popped from payment_request_dialog_view's view

stack, the key-pair will be destroyed. If the controller doesn't reset
WebContentsModalDialogManager's delegate in the controller's destructor,
the WebView's destructor will attempt to access into
WebContentsModalDialogManager's delegate, and cause a use-after-free
crash.

This CL fixes this issue by making sure
PaymentHandlerWebFlowViewController's destructor resets
WebContentsModalDialogManager's delegate.

(cherry picked from commit 8f6ad3de87d3d7b375f75004b1389604887d31fb)

(cherry picked from commit 3e2beb764726f0e0a151af76910e189bafbaa97d)

~~Bug: 1194958~~
Change-Id: Iead54db4b3e682bbccccddf335780c5ceff2e990
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2844509
Commit-Queue: Liquan (Max) Gu <maxlg@chromium.org>
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#875868}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2849774
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1388}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884069
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#21}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/a5c6b0255c70aec702bf9952117063549679cf29/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 85 by gianluca@google.com on Wed, May 12, 2021, 12:34 PM EDT

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

Comment 86 by Git Watcher on Wed, May 12, 2021, 2:35 PM EDT

**Labels:** merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/202bf9af3e4cb2039e73950afd36689e03585845

commit 202bf9af3e4cb2039e73950afd36689e03585845
Author: Liquan (Max) Gu <maxlg@chromium.org>
Date: Wed May 12 18:34:14 2021

Clean up WebContentsModalDialogManagerDelegate in desktop Payment UI

payment_request_dialog_view's controller_map_ store the
PaymentHandlerWebFlowViewController and its web-view as a key-value
pair. When the view is popped from payment_request_dialog_view's view
stack, the key-pair will be destroyed. If the controller doesn't reset
WebContentsModalDialogManager's delegate in the controller's destructor,
the WebView's destructor will attempt to access into
WebContentsModalDialogManager's delegate, and cause a use-after-free
crash.

This CL fixes this issue by making sure
PaymentHandlerWebFlowViewController's destructor resets
WebContentsModalDialogManager's delegate.

(cherry picked from commit 8f6ad3de87d3d7b375f75004b1389604887d31fb)

~~Bug: 1194958~~
Change-Id: Iead54db4b3e682bbccccddf335780c5ceff2e990
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2844509
Commit-Queue: Liquan (Max) Gu <maxlg@chromium.org>
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#875868}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883622
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1637}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/202bf9af3e4cb2039e73950afd36689e03585845/chrome/browser/ui/views/payments/payment_handler_web_flow_view_controller.cc

Comment 87 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT

**Labels:** -CVE_description-missing CVE_description-submitted

Comment 88 by sheriffbot on Thu, Aug 19, 2021, 1:30 PM EDT

**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