





☆ Starred by 4 users

Owner:	<div> sahel@chromium.org</div> <div>Last visit > 30 days ago</div>
CC:	<div>adetaylor@chromium.org</div> <div>rouslan@chromium.org</div> <div> danyao@chromium.org</div> <div>janag...@google.com</div> <div> maxlg@chromium.org</div> <div> marinakz@chromium.org</div>
Status:	Fixed (Closed)
Components:	Blink>Payments
Modified:	May 4, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-01-22
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security
<div>Security_Impact-Stable</div> <div>Hotlist-Merge-Approved</div> <div>Security_Severity-High</div> <div>allpublic</div> <div>reward-inprocess</div> <div>reward-15000</div> <div>CVE_description-submitted</div> <div>M-89</div> <div>Target-89</div> <div>merge-merged-4240</div> <div>merge-merged-86</div> <div>LTR-Merged-86</div> <div>LTS-Security-86</div> <div>merge-merged-4324</div> <div>merge-merged-88</div> <div>external_security_report</div> <div>merge-merged-4389</div> <div>merge-merged-89</div> <div>Release-3-M88</div> <div>CVE-2021-21151</div>	

Issue 1165624: Security: UaF in chrome!payments::PaymentRequestSheetController::UpdateHeaderView

Reported by chrom...@gmail.com on Mon, Jan 11, 2021, 11:11 PM EST

 Code

Description #2 by sahel@chromium.org (Jan 18, 2021)

VERSION
Chrome Version: 89.0.4384.0 (Official Build) canary (x86_64)
Operating System: MacOS and Windows

REPRODUCTION CASE
0. ensure that #enable-portals and #enable-portals-cross-origin from chrome://flags are enabled.
1. go to <http://localhost:8000/repro.html>
2. Open another tab and go to <https://maxlgu.github.io/pr/max-nonbasiccard/>
3. Click on "Busy" button.
4. In payments window try to change <http://www.google.com> to <http://localhost:8000/repro.html> then click on "Go!" button.
5. Navigate backward

Crash/3b2d5b5dfda73019.

```
*** WARNING: Unable to verify checksum for chrome.dll
rax=efefefefefefefef rbx=000076d0012d3800 rcx=000076d000bf8c50
rdx=30335b0200000001 rsi=000076d000bf8c50 rdi=000076d000ea24f8
rip=00007fa6645ba4b rsp=000000c17c3fc6e0 rbp=aaaaaaaaaaaaaaaa
r8=0000000000000080 r9=00000000ff000000 r10=00000000ff000000
r11=8101010101010100 r12=0000000000000000 r13=aaaaaaaaaaaaaaaa
r14=000076d000ea24d0 r15=aaaaaaaaaaaaaaaa
iopl=0         nv up ei pl zr na po nc
cs=0033  ss=0000  ds=0000  es=0000  fs=0053  gs=002b             efl=00010246
chrome!views::View::UpdateTooltip+0x6 [inlined in chrome!views::View::RemoveAllChildViews+0x4b]:
00007fa6645ba4b ff5050      call     qword ptr [rax+50h]:ds:efefefefefef03f=????????????????
0:000> k
*** Stack trace for last set context - .thread!cxr resets it
# Child-SP      RetAddr      Call Site
00 (Inline Function) ----- chrome!views::View::UpdateTooltip+0x6 [c:\b\sw\cache\builder\src\ui\views\view.cc @ 3083]
01 000000c1'7c3fc6e0 00007fa'6cc335f8 chrome!views::View::RemoveAllChildViews+0x4b [c:\b\sw\cache\builder\src\ui\views\view.cc @ 298]
02 000000c1'7c3fc720 00007fa'66dc4552 chrome!payments::PaymentRequestSheetController::UpdateHeaderView+0x28
[c:\b\sw\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc @ 298]
03 000000c1'7c3fc7a0 00007fa'6b4e6b18 chrome!content::WebContentsImpl::DidChangeVisibleSecurityState+0x72
[c:\b\sw\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 2348]
04 000000c1'7c3fc900 00007fa'67bb2b1f chrome!security_interstitials::SecurityInterstitialTabHelper::DidFinishNavigation+0xd8
[c:\b\sw\cache\builder\src\components\security_interstitials\content\security_interstitial_tab_helper.cc @ 43]
05 (Inline Function) ----- chrome!content::WebContentsImpl::DidFinishNavigation:<unnamed-tag>::operator()+0xf
[c:\b\sw\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 5167]
06 (Inline Function) ----- chrome!content::WebContentsImpl::WebContentsObserverList::ForEachObserver+0x237
[c:\b\sw\cache\builder\src\content\browser\web_contents\web_contents_impl.h @ 1447]
07 000000c1'7c3fc960 00007fa'662a6548 chrome!content::WebContentsImpl::DidFinishNavigation+0x29f
[c:\b\sw\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 5166]
```

```
08 000000c1'7c3fca0 00007ffa'662a63d0 chrome!content:NavigationRequest::~NavigationRequest+0x158
[c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc @ 1338]
09 000000c1'7c3fcc90 00007ffa'65623ce7 chrome!content:NavigationRequest::~NavigationRequest+0x10
[c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc @ 1296]
0a (Inline Function) ----- chrome!std::_1::default_delete<media::RendererFactory>::operator()()+0xa
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2378]
0b (Inline Function) ----- chrome!std::_1::unique_ptr<media::RendererFactory,std::default_delete<media::RendererFactory>>::reset()+0x1b
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2633]
0c (Inline Function) ----- chrome!std::_1::unique_ptr<media::RendererFactory,std::default_delete<media::RendererFactory>>::~unique_ptr+0x1b
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2587]
0d (Inline Function) ----- chrome!std::_1::pair<const
media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delete<media::RendererFactory>>>::pair+0x1b
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\utility @ 297]
0e (Inline Function) -----
chrome!std::_1::allocator_traits<std::allocator<std::_tree_node<std::_value_type<media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delet
e<media::RendererFactory>>>,void*>>::destroy()+0x1b [c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 1787]
0f (Inline Function) -----
chrome!std::_1::allocator_traits<std::allocator<std::_tree_node<std::_value_type<media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delet
e<media::RendererFactory>>>,void*>>::destroy()+0x1b [c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 1619]
10 000000c1'7c3fcd0 00007ffa'66d9a0a6
chrome!std::_1::tree<std::_value_type<media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delete<media::RendererFactory>>>
,std::_map_value_compare<media::RendererFactoryType,std::_value_type<media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delete<m
edia::RendererFactory>>>>>
>,std::less<media::RendererFactoryType>,1>,std::allocator<std::_value_type<media::RendererFactoryType,std::unique_ptr<media::RendererFactory,std::default_delete<m
edia::RendererFactory>>>>> >> >>::destroy()+0x47 [c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\_tree @ 1831]
11 (Inline Function) ----- chrome!std::_1::tree<std::_value_type<content:NavigationRequest
*,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>>,std::_map_value_compare<content:NavigationRequest
*,std::_value_type<content:NavigationRequest*,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>>
>,std::less<content:NavigationRequest*,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>>
>,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>> >> >>::clear()+0x13
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\_tree @ 1870]
12 (Inline Function) ----- chrome!std::_1::map<content:NavigationRequest
*,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>,std::less<content:NavigationRequest
*,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>> >,std::allocator<std::pair<content:NavigationRequest*,const,std::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>>>>
>>::clear()+0x13 [c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\map @ 1309]
13 000000c1'7c3fcd10 00007ffa'66b292df chrome!content:RenderFrameHostImpl::ResetNavigationRequests()+0x26
[c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc @ 3275]
14 000000c1'7c3fcd60 00007ffa'66b28d10 chrome!content:WebContentsImpl::~WebContentsImpl+0x5af
[c:\b\sw\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 956]
15 000000c1'7c3fcd30 00007ffa'66056e8c chrome!content:WebContentsImpl::~WebContentsImpl+0x10
[c:\b\sw\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 868]
16 (Inline Function) ----- chrome!std::_1::default_delete<content:WebContents>::operator()()+0xa
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2378]
17 (Inline Function) ----- chrome!std::_1::unique_ptr<content:WebContents,std::default_delete<content:WebContents>>::reset()+0x128
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2633]
18 000000c1'7c3cf70 00007ffa'665cf316 chrome!views:WebView::SetWebContents()+0x1dc [c:\b\sw\ir\cache\builder\src\ui\views\controls\webview\webview.cc @ 97]
19 000000c1'7c3fd020 00007ffa'665cf240 chrome!views:WebView::~WebView+0xb6 [c:\b\sw\ir\cache\builder\src\ui\views\controls\webview\webview.cc @ 72]
1a 000000c1'7c3fd070 00007ffa'65afa07f chrome!views:WebView::~WebView+0x10 [c:\b\sw\ir\cache\builder\src\ui\views\controls\webview\webview.cc @ 69]
1b 000000c1'7c3fd0b0 00007ffa'66f7a320 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
1c 000000c1'7c3fd1b0 00007ffa'65afa07f chrome!views:View::~View+0x10 [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 203]
1d 000000c1'7c3fd1f0 00007ffa'66f7a320 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
1e 000000c1'7c3fd2f0 00007ffa'65afa07f chrome!views:View::~View+0x10 [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 203]
1f 000000c1'7c3fd330 00007ffa'6ac7f150 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
20 (Inline Function) ----- chrome!views:ScrollView::Viewport::~Viewport+0x95 [c:\b\sw\ir\cache\builder\src\ui\views\controls\scroll_view.cc @ 133]
21 000000c1'7c3fd430 00007ffa'65afa07f chrome!views:ScrollView::Viewport::~Viewport+0xa0 [c:\b\sw\ir\cache\builder\src\ui\views\controls\scroll_view.cc @ 133]
22 000000c1'7c3fd470 00007ffa'6ac7fec0 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
23 000000c1'7c3fd570 00007ffa'65afa07f chrome!views:ScrollView::ScrollView+0x10 [c:\b\sw\ir\cache\builder\src\ui\views\controls\scroll_view.cc @ 238]
24 000000c1'7c3fd5b0 00007ffa'67722a67 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
25 (Inline Function) ----- chrome!payments::anonymous namespace::SheetView::~SheetView+0xdc
[c:\b\sw\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc @ 57]
26 000000c1'7c3fd6b0 00007ffa'65afa07f chrome!payments::anonymous namespace::SheetView::~SheetView+0xe7
[c:\b\sw\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_sheet_controller.cc @ 57]
27 000000c1'7c3fd6f0 00007ffa'6c3c2c90 chrome!views:View::~View+0x18f [c:\b\sw\ir\cache\builder\src\ui\views\view.cc @ 220]
28 000000c1'7c3fd7f0 00007ffa'6c9b4d32 chrome!ViewStack::~ViewStack+0x10 [c:\b\sw\ir\cache\builder\src\chrome\browser\ui\views\payments\view_stack.cc @ 30]
29 (Inline Function) ----- chrome!std::_1::default_delete<ViewStack>::operator()()+0xe
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2378]
2a (Inline Function) ----- chrome!std::_1::unique_ptr<ViewStack,std::default_delete<ViewStack>>::reset()+0x10
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2633]
2b (Inline Function) ----- chrome!std::_1::unique_ptr<ViewStack,std::default_delete<ViewStack>>::~unique_ptr+0x10
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2587]
2c 000000c1'7c3fd830 00007ffa'67954b5e chrome!payments::PaymentRequestDialogView::OnDialogClosed()+0x62
[c:\b\sw\ir\cache\builder\src\chrome\browser\ui\views\payments\payment_request_dialog_view.cc @ 98]
2d (Inline Function) ----- chrome!base::internal::InvokeHelper<1,void>::MakeItSo()+0x42 [c:\b\sw\ir\cache\builder\src\base\bind_internal.h @ 657]
2e (Inline Function) ----- chrome!base::internal::Invoker<base::internal::BindState,void (net::MDnsListenerImpl::*)(),base::WeakPtr<net::MDnsListenerImpl>>::void
()>::RunImpl()+0x42 [c:\b\sw\ir\cache\builder\src\base\bind_internal.h @ 710]
2f 000000c1'7c3fd880 00007ffa'690bc440 chrome!base::internal::Invoker<base::internal::BindState<void (net::MDnsListenerImpl::*)
()>,base::WeakPtr<net::MDnsListenerImpl>>>::void()>::Run()+0x5e [c:\b\sw\ir\cache\builder\src\base\bind_internal.h @ 695]
30 (Inline Function) ----- chrome!base::OnceCallback<void()>::Run()+0x11 [c:\b\sw\ir\cache\builder\src\base\callback.h @ 101]
31 (Inline Function) ----- chrome!views::DialogDelegate::RunCloseCallback()+0x1d [c:\b\sw\ir\cache\builder\src\ui\views\window\dialog_delegate.cc @ 172]
32 000000c1'7c3fd8d0 00007ffa'6664ff48 chrome!views::DialogDelegate::WindowWillClose()+0x80 [c:\b\sw\ir\cache\builder\src\ui\views\window\dialog_delegate.cc @ 232]
33 (Inline Function) ----- chrome!base::OnceCallback<void()>::Run()+0x25 [c:\b\sw\ir\cache\builder\src\base\callback.h @ 101]
34 000000c1'7c3fd920 00007ffa'6664fd03 chrome!views::WidgetDelegate::WindowWillClose()+0x68 [c:\b\sw\ir\cache\builder\src\ui\views\widget\widget_delegate.cc @
211]
35 000000c1'7c3fd980 00007ffa'670c016c chrome!views::Widget::CloseWithReason()+0x2e3 [c:\b\sw\ir\cache\builder\src\ui\views\widget\widget.cc @ 630]
36 (Inline Function) ----- chrome!web_modal::WebContentsModalDialogManager::CloseAllDialogs()+0x2d
[c:\b\sw\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc @ 124]
37 000000c1'7c3fda60 00007ffa'67bb2b1f chrome!web_modal::WebContentsModalDialogManager::DidFinishNavigation()+0x8c
[c:\b\sw\ir\cache\builder\src\components\web_modal\web_contents_modal_dialog_manager.cc @ 136]
38 (Inline Function) ----- chrome!content:WebContentsImpl::DidFinishNavigation():<unnamed-tag>::operator()()+0xf
[c:\b\sw\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 5167]
39 (Inline Function) ----- chrome!content:WebContentsImpl::WebContentsObserverList::ForEachObserver()+0x237
[c:\b\sw\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.h @ 1447]
3a 000000c1'7c3fdaa0 00007ffa'662a6548 chrome!content:WebContentsImpl::DidFinishNavigation()+0x29f
[c:\b\sw\ir\cache\builder\src\content\browser\web_contents\web_contents_impl.cc @ 5166]
3b 000000c1'7c3fdc00 00007ffa'662a63d0 chrome!content:NavigationRequest::~NavigationRequest+0x158
[c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc @ 1338]
3c 000000c1'7c3fdd0 00007ffa'65d4b581 chrome!content:NavigationRequest::~NavigationRequest+0x10
[c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc @ 1296]
3d (Inline Function) ----- chrome!std::_1::default_delete<content:NavigationRequest>::operator()()+0xa
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2378]
3e (Inline Function) ----- chrome!std::_1::unique_ptr<content:NavigationRequest,std::default_delete<content:NavigationRequest>>::reset()+0x19
[c:\b\sw\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\memory @ 2633]
3f 000000c1'7c3fde10 00007ffa'65d48d39 chrome!content:Navigator::DidNavigate()+0x671 [c:\b\sw\ir\cache\builder\src\content\browser\renderer_host\navigator.cc @
```

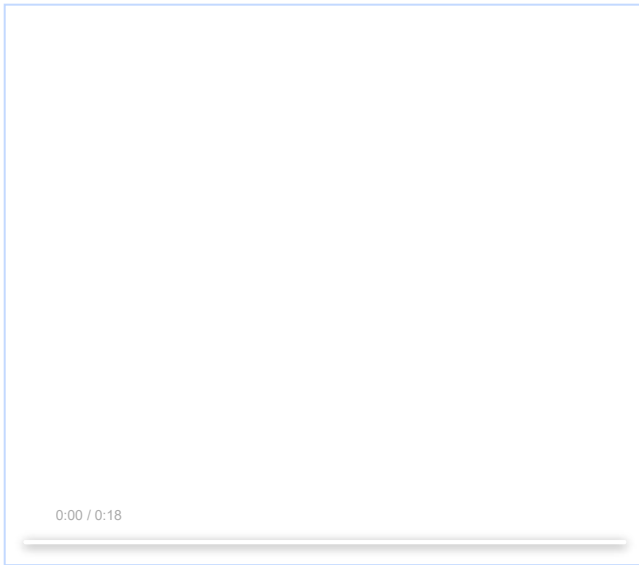
```
420]
40 000000c17c3fe030 00007ffa662261f1 chromelcontent::RenderFrameHostImpl::DidCommitNavigationInternal+0x429
[c:\b\sl\w\i\c\ac\h\builder\src\content\b\browser\renderer_host\renderer_frame_host_impl.cc @ 8884]
41 0000000c17c3fe1f0 00007ffa66225dc9 chromelcontent::RenderFrameHostImpl::DidCommitNavigation+0x411
[c:\b\sl\w\i\c\ac\h\builder\src\content\b\browser\renderer_host\renderer_frame_host_impl.cc @ 9337]
42 (Inline Function) ----- chromelbase::internal::FunctorTraits<void (content::RenderFrameHostImpl::*)(content::NavigationRequest *,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>, mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>),void>::Invoke+0x2d
[c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 498]
43 (Inline Function) ----- chromelbase::internal::InvokeHelper<0,void>::MakeItSo+0x35 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 637]
44 (Inline Function) ----- chromelbase::internal::Invoker<base::internal::BindState+void (content::RenderFrameHostImpl::*)(content::NavigationRequest *,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>),base::internal::UnretainedWrapper<content::RenderFrameHostImpl>,content::NavigationRequ
est*>::void (mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>)>::RunImpl+0x35 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 710]
45 0000000c17c3fe380 00007ffa661b0e99 chromelbase::internal::Invoker<base::internal::BindState+void (content::RenderFrameHostImpl::*)(content::NavigationRequest
*, mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>),base::internal::UnretainedWrapper<content::RenderFrameHostImpl>,content::NavigationRequ
est*>::void (mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>)>::RunOnce+0x49 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 679]
46 (Inline Function) ----- chromelbase::OnceCallback<void (mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,
mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>)>::Run+0xd [c:\b\sl\w\i\c\ac\h\builder\src\base\callback.h @ 101]
47 0000000c17c3fe3d0 00007ffa689747f6 chromelcontent::mojom::NavigationClient_CommitNavigation_ForwardToCallback::Accept+0x179
[c:\b\sl\w\i\c\ac\h\builder\src\out\Release_x64\gen\content\common\navigation_client.mojom.cc @ 652]
48 0000000c17c3fe4d0 00007ffa68aabe4d chromelmojom::InterfaceEndpointClient::HandleValidatedMessage+0x2b6
[c:\b\sl\w\i\c\ac\h\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc @ 549]
49 0000000c17c3fe580 00007ffa68aabd20 chromelIPC::anonymous namespace::ChannelAssociatedGroupController::AcceptOnProxyThread+0x10d
[c:\b\sl\w\i\c\ac\h\builder\src\ipc\ipc_mojom_bootstrap.cc @ 946]
4a (Inline Function) ----- chromelbase::internal::FunctorTraits<void (IPC:::(anonymous namespace)::ChannelAssociatedGroupController::*)(
mojo::Message),void>::Invoke+0x69 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 498]
4b (Inline Function) ----- chromelbase::internal::InvokeHelper<0,void>::MakeItSo+0x71 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 637]
4c (Inline Function) ----- chromelbase::internal::Invoker<base::internal::BindState+void (IPC:::(anonymous namespace)::ChannelAssociatedGroupController::*)(
mojo::Message),scoped_refptr<IPC:::(anonymous namespace)::ChannelAssociatedGroupController>,mojo::Message>,void (*)>::RunImpl+0x75
[c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 710]
4d 0000000c17c3fe650 00007ffa687f9849 chromelbase::internal::Invoker<base::internal::BindState+void (IPC:::(anonymous
namespace)::ChannelAssociatedGroupController::*)(mojo::Message),scoped_refptr<IPC:::(anonymous
namespace)::ChannelAssociatedGroupController>,mojo::Message>,void (*)>::RunOnce+0x90 [c:\b\sl\w\i\c\ac\h\builder\src\base\bind_internal.h @ 683]
4e (Inline Function) ----- chromelbase::OnceCallback<void (*)>::Run+0x15 [c:\b\sl\w\i\c\ac\h\builder\src\base\callback.h @ 101]
4f 0000000c17c3fe710 00007ffa67f9e1bf chromelbase::TaskAnnotator::RunTask+0x169 [c:\b\sl\w\i\c\ac\h\builder\src\base\task\common\task_annotator.cc @ 163]
50 0000000c17c3fe850 00007ffa67f9de3c chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl+0x1df
[c:\b\sl\w\i\c\ac\h\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 352]
51 0000000c17c3fea40 00007ffa68c2e676 chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork+0xc
[c:\b\sl\w\i\c\ac\h\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 266]
52 0000000c17c3feae0 00007ffa67e45ebe chromelbase::MessagePumpForUI::DoRunLoop+0x76
[c:\b\sl\w\i\c\ac\h\builder\src\base\message_loop\message_pump_win.cc @ 225]
53 0000000c17c3feb70 00007ffa65d342ec chromelbase::MessagePumpWin::Run+0xc [c:\b\sl\w\i\c\ac\h\builder\src\base\message_loop\message_pump_win.cc @ 82]
54 0000000c17c3febe0 00007ffa65a7b386 chromelbase::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0x7c
[c:\b\sl\w\i\c\ac\h\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 463]
55 0000000c17c3fec40 00007ffa6671949b chromelbase::RunLoop::Run+0xb6 [c:\b\sl\w\i\c\ac\h\builder\src\base\run_loop.cc @ 133]
56 0000000c17c3fed10 00007ffa663ac07b chromelChromeBrowserMainParts::MainMessageLoopRun+0xdb
[c:\b\sl\w\i\c\ac\h\builder\src\chromel\browser\chrome_browser_main.cc @ 1739]
57 0000000c17c3feda0 00007ffa663ac051 chromelcontent::BrowserMainLoop::RunMainMessageLoopParts+0xb
[c:\b\sl\w\i\c\ac\h\builder\src\content\b\browser\browser_main_loop.cc @ 976]
58 0000000c17c3fedd0 00007ffa67afcb43 chromelcontent::BrowserMainRunnerImpl::Run+0x11
[c:\b\sl\w\i\c\ac\h\builder\src\content\b\browser\browser_main_runner_impl.cc @ 151]
59 0000000c17c3fee00 00007ffa67e39772 chromelcontent::BrowserMain+0xe3 [c:\b\sl\w\i\c\ac\h\builder\src\content\b\browser\browser_main.cc @ 47]
5a (Inline Function) ----- chromelcontent::RunBrowserProcessMain+0x43 [c:\b\sl\w\i\c\ac\h\builder\src\content\app\content_main_runner_impl.cc @ 555]
5b 0000000c17c3feaa0 00007ffa67e3934a chromelcontent::ContentMainRunnerImpl::RunBrowser+0x3f2
[c:\b\sl\w\i\c\ac\h\builder\src\content\app\content_main_runner_impl.cc @ 1059]
5c 0000000c17c3fefaa0 00007ffa65c64ef9 chromelcontent::ContentMainRunnerImpl::Run+0x14a [c:\b\sl\w\i\c\ac\h\builder\src\content\app\content_main_runner_impl.cc @
929]
5d 0000000c17c3ff040 00007ffa65c63acd chromelcontent::RunContentProcess+0x3c9 [c:\b\sl\w\i\c\ac\h\builder\src\content\app\content_main.cc @ 372]
5e 0000000c17c3ff250 00007ffa65c638fc chromelcontent::ContentMain+0x3d [c:\b\sl\w\i\c\ac\h\builder\src\content\app\content_main.cc @ 398]
5f 0000000c17c3ff2a0 00007ffa6257d15eb chromelChromeMain+0x18c [c:\b\sl\w\i\c\ac\h\builder\src\chrome\app\chrome_main.cc @ 144]
60 0000000c17c3ff3c0 00007ffa6257d1194 chrome_exe!GetHandleVerifier+0x1bebb
61 0000000c17c3ff490 00007ffa625859ae2 chrome_exe!GetHandleVerifier+0x1ba64
*** WARNING: Unable to verify checksum for KERNEL32.DLL
62 0000000c17c3ff880 00007ffa9a946fd4 chrome_exe!IsSandboxedProcess+0x85122
63 0000000c17c3ff8c0 00007ffa9aa7cec1 KERNEL32!BaseThreadInitThunk+0x14
64 0000000c17c3ff8f0 0000000000000000 ntdll!IRtlUserThreadStart+0x21
```

repro.html

379 bytes [View](#) [Download](#)

screen.mov

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



Comment 1 Deleted

Comment 2 by [sheriffbot](#) on Mon, Jan 11, 2021, 11:12 PM EST

Labels: reward-potential

Comment 3 by [chrom...@gmail.com](#) on Mon, Jan 11, 2021, 11:12 PM EST

This is similar to [issue-1114556](#).

Comment 4 by [xinghuilu@chromium.org](#) on Tue, Jan 12, 2021, 5:49 PM EST

Status: Assigned (was: Unconfirmed)

Owner: [sahel@chromium.org](#)

Cc: [rouslan@chromium.org](#) [maxlg@chromium.org](#)

Labels: Security_Severity-High Security_Impact-Head OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1

Components: Blink>Payments

Thanks for the report! And thanks for providing extra pointer to <https://crbug.com/1114556>. [sahel@](#), could you take a look at this crash too? Thanks!

link to the crash: <https://crash.corp.google.com/browse?q=ReportID%3D%273b2d5b5dfda73019%27&stbtq=&reportid=&index=0>

Comment 5 by [rouslan@chromium.org](#) on Wed, Jan 13, 2021, 9:00 AM EST

NextAction: 2021-01-15

Comment 6 by [sheriffbot](#) on Thu, Jan 14, 2021, 12:52 PM EST

Labels: Target-89 M-89

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

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

Comment 7 by [sheriffbot](#) on Thu, Jan 14, 2021, 1:18 PM EST

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 8 by [monor...@bugs.chromium.org](#) on Fri, Jan 15, 2021, 7:00 AM EST

The NextAction date has arrived: 2021-01-15

Comment 9 by [sahel@chromium.org](#) on Mon, Jan 18, 2021, 10:59 AM EST

Cc: [danyao@chromium.org](#)

Labels: Needs-Feedback

I cannot reproduce the issue using the steps in the bug description. (I tried both Windows and Linux, also Chrome Stable and Dev 89.0.4385.0)

Please see the recording attached.

By looking at the crash trace I have a tentative fix, however I cannot confirm it without being able to repro the issue.

[chromium.khali@](#) could you please answer the following questions?

1-Are you able to produce the issue deterministically?

2-Is the issue reproducible on Chrome Stable?

3-Have you made any changes in `chrome://flags`?

Comment 10 by [sahel@chromium.org](#) on Mon, Jan 18, 2021, 11:01 AM EST

Forgot to add the video in [comment #9](#). Actually attaching it here.

repro.mkv

1.8 MB [Download](#)

Comment 11 by [sahel@chromium.org](#) on Mon, Jan 18, 2021, 11:17 AM EST

[chromium.khali@](#) the bug description suggests that the issue happens on Mac and Windows. The recording however looks like to be from Mac?

Could you please confirm whether or not the issue is reproducible on Windows?

Comment 12 by [chrom...@gmail.com](#) on Mon, Jan 18, 2021, 11:29 AM EST

Hmm... you need to enable `chrome://flags/#enable-portals` and `chrome://flags/#enable-portals-cross-origin`.

Comment 13 by chrom...@gmail.com on Mon, Jan 18, 2021, 11:34 AM EST

1-Are you able to produce the issue deterministically?
> Yes
2-Is the issue reproducible on Chrome Stable?
> Yes
3-Have you made any changes in chrome://flags?
enable #enable-portals and #enable-portals-cross-origin

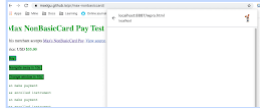
I was able to repro this on Windows.

Comment 14 by maxlg@chromium.org on Mon, Jan 18, 2021, 11:38 AM EST

Sahel, try enabling the two "portals" flags in about://flags. I could reproduce it with the two flags enabled.

Screen Shot 2021-01-18 at 11.26.25.png

81.2 KB View Download



Comment 15 by sahel@chromium.org on Mon, Jan 18, 2021, 12:20 PM EST

Labels: -Needs-Feedback Security_Needs_Attention-Severity

Thank you chromium.khalil@ for the prompt response and maxlg@ for trying the repro with and without the flags.

I confirm that with #enable-portals and #enable-portals-cross-origin flags enabled I can reproduce the issue. Since the issue is only reproducible by enabling portal flags and is not a recent regression (reproducible on current Chrome stable) I don't think it should be a release blocker, I also don't think it has high security severity.

Comment 16 by sahel@chromium.org on Mon, Jan 18, 2021, 12:21 PM EST

Description was changed.

Comment 17 by chrom...@gmail.com on Mon, Jan 18, 2021, 12:29 PM EST

Sometimes, I can repro it without enabling flags with using <https://lbstyle.github.io/o.html> (It does take several attempts to repro)

Comment 18 by bugdroid on Tue, Jan 19, 2021, 2:35 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+a1a3f9552ce156e3cc3bd0207e53b78609e4b07a>

commit a1a3f9552ce156e3cc3bd0207e53b78609e4b07a

Author: Sahel Sharify <sahel@chromium.org>

Date: Tue Jan 19 19:34:07 2021

[Web Payment]PR_sheet_controller should not update views during PR abort

Similar to <https://bugs.chromium.org/p/chromium/issues/detail?id=993223>

PaymentRequestSheetController::UpdateHeaderView gets called after the payment request(PR) has been aborted. The fix for <https://bugs.chromium.org/p/chromium/issues/detail?id=993223> early returns in DidFinishNavigation which is the caller of UpdateHeaderView.

That's why calling UpdateHeaderView from a different function (e.g. DidChangeVisibleSecurityState in the case of <https://bugs.chromium.org/p/chromium/issues/detail?id=1465624>) still reproduces the issue.

This CL early returns in all PaymentRequestSheetController's Update...View functions when the PR is being aborted.

[Bug-1465624](https://bugs.chromium.org/p/chromium/issues/detail?id=1465624)

Change-Id: Ie6f8f8ff6e72ef16878aa8dc3f15e19dea1587e1

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2635074>

Reviewed-by: Rouslan Solomakhin <rousian@chromium.org>

Commit-Queue: Sahel Sharify <sahel@chromium.org>

Cr-Commit-Position: refs/heads/master@{#844843}

[modify] https://crrev.com/a1a3f9552ce156e3cc3bd0207e53b78609e4b07a/chrome/browser/ui/views/payments/payment_request_sheet_controller.cc

Comment 19 by chrom...@gmail.com on Wed, Jan 20, 2021, 10:28 AM EST

Unable to repro this on Canary 90.0.4394.0. Fixed.

Comment 20 by sahel@chromium.org on Wed, Jan 20, 2021, 11:08 AM EST

Status: Started (was: Assigned)

NextAction: 2021-01-22

Thank you chromium.khalil@ for confirming the fix.

The fix in [comment #18](#) is first landed in 90.0.4394.0 on which the reporter has confirmed the fix. I let the code to be in Canary for 2 days and will merge request to M89 on Friday.

Comment 21 by sheriffbot on Wed, Jan 20, 2021, 12:21 PM EST

Labels: -Security_Impact-Head Security_Impact-Beta

Comment 22 by adetaylor@google.com on Wed, Jan 20, 2021, 6:57 PM EST

Labels: -reward-potential external_security_report

Comment 23 by monor...@bugs.chromium.org on Fri, Jan 22, 2021, 7:00 AM EST

The NextAction date has arrived: 2021-01-22

Comment 24 by sahel@chromium.org on Fri, Jan 22, 2021, 11:14 AM EST

Labels: Merge-Request-89

I request to merge the fix in [comment #18](#) to M89. The fix has been in Canary for two days.

Comment 25 by sheriffbot on Sat, Jan 23, 2021, 11:20 AM EST

Labels: -Merge-Request-89 Hotlist-Merge-Approved Merge-Approved-89

Your change meets the bar and is auto-approved for M89. Please go ahead and merge the CL to branch 4389 (refs/branch-heads/4389) manually. Please contact milestone owner if you have questions.

Merge instructions: <https://www.chromium.org/developers/how-tos/drover>

Owners: benmason@ (Android), bindusuvama@ (iOS), geohsu@ (ChromeOS), pbommana@ (Desktop)

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

Comment 26 by [pbommana@google.com](#) on Sun, Jan 24, 2021, 11:48 PM EST

[Bulk Edit]Please go ahead and merge the CL to branch 4389 (refs/branch-heads/4389) manually, So that the change would be picked as part of this week Dev release.

Comment 27 by [bugdroid](#) on Mon, Jan 25, 2021, 11:39 AM EST

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+1b5af00432c9cff1670b7e4d9565f2f1b881cb7d>

commit 1b5af00432c9cff1670b7e4d9565f2f1b881cb7d

Author: Sahel Sharify <sahel@chromium.org>

Date: Mon Jan 25 16:38:35 2021

[Merge M-89][Web Payment]PR_sheet_controller should not update views during PR abort

Similar to [crbug.com/993223](#)

PaymentRequestSheetController::UpdateHeaderView gets called after the payment request(PR) has been aborted. The fix for [crbug.com/993223](#) early returns in DidFinishNavigation which is the caller of UpdateHeaderView.

That's why calling UpdateHeaderView from a different function (e.g. DidChangeVisibleSecurityState in the case of [crbug.com/1165624](#)) still reproduces the issue.

This CL early returns in all PaymentRequestSheetController's Update...View functions when the PR is being aborted.

(cherry picked from commit [a1a3f9552ce156e3cc3bd0207e53b78609e4b07a](#))

[Bug-1165624](#)

Change-Id: Ie6f8f8ff6e72ef16878aa8dc3f15e19dea1587e1

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2635074>

Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>

Commit-Queue: Sahel Sharify <sahel@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#844843}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2647645>

Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>

Cr-Commit-Position: refs/branch-heads/4389@{#200}

Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/1b5af00432c9cff1670b7e4d9565f2f1b881cb7d/chrome/browser/ui/views/payments/payment_request_sheet_controller.cc

Comment 28 by [danyao@chromium.org](#) on Mon, Jan 25, 2021, 3:06 PM EST

Status: Fixed (was: Started)

Marking fixed since the change has been merged. I'll verify the change once it's in Dev.

Comment 29 by [sheriffbot](#) on Tue, Jan 26, 2021, 12:45 PM EST

Labels: reward-topanel

Comment 30 by [sheriffbot](#) on Tue, Jan 26, 2021, 2:00 PM EST

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

Comment 31 by [adetaylor@google.com](#) on Wed, Feb 10, 2021, 12:37 PM EST

Cc: adetaylor@chromium.org

sahel@ as I understand it, Portals was in an origin trial which is no longer active (per [issue-1158376](#)). Is that the case? If so I'd like to update the Security_Impact label here to None, which will affect what we do in terms of release notes, CVE filing and merges. Please confirm. Thanks!

(It would remain High severity; possibly even Critical, but as it would be impact None this would make little difference to anything).

Comment 32 by [adetaylor@google.com](#) on Wed, Feb 10, 2021, 12:38 PM EST

sahel@ please also confirm that this is entirely dependent on Portals and there's no chance that this is exploitable without Portals being enabled.

Comment 33 by [sahel@chromium.org](#) on Wed, Feb 10, 2021, 1:13 PM EST

The reproduction case from bug report does needs #enable-portals and #enable-portals-cross-origin flags enabled. However per reporter's [comment #17](#) the issue is reproducible on <https://lifestyle.github.io/o.html> without enabling portal flags (several attempts needed).

That being said I cannot confirm that the issue is entirely dependent on Portals.

Comment 34 by [amyressler@google.com](#) on Wed, Feb 10, 2021, 1:59 PM EST

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 35 by [amyressler@google.com](#) on Wed, Feb 10, 2021, 3:55 PM EST

Congratulations, Khalil - the VRP Panel has decided to award you \$15,000 for this report. Nice work!

Comment 36 by [adetaylor@google.com](#) on Wed, Feb 10, 2021, 4:03 PM EST

Thanks sahel@. chromium.khalil@, and sahel@, do either of you have an idea whether this is reproducible on M88? (even sometimes?)

Comment 37 by [sahel@chromium.org](#) on Wed, Feb 10, 2021, 4:05 PM EST

Yes it is reproducible on M88 since the fix is merged to M89 only.

Comment 38 by [adetaylor@chromium.org](#) on Wed, Feb 10, 2021, 4:11 PM EST

Labels: -Security_Severity-High -Security_Impact-Beta -ReleaseBlock-Stable -Security_Needs_Attention-Severity Security_Impact-Stable Security_Severity-Critical Merge-Approved-88

Thanks.

In that case:

- adjusting impact to Security_Impact-Stable
- adjusting severity to Critical, since this appears to be browser process memory corruption directly achievable from HTML content with no UI interaction
- approving merge to M88, branch 4389. Please go ahead and merge sometime before the end of Thursday PST, so we can get this into next week's stable refresh.

[Comment 39](#) by [adetaylor@google.com](#) on Wed, Feb 10, 2021, 4:16 PM EST

Labels: -Security_Severity-Critical Security_Severity-High

sahel@ has pointed out that all known repros do involve a user gesture, so bumping down to High again.

[Comment 40](#) by [sahel@chromium.org](#) on Wed, Feb 10, 2021, 4:17 PM EST

Yes, a user gesture is mandatory for triggering payment request UI.

[Comment 41](#) by [bugdroid](#) on Wed, Feb 10, 2021, 5:24 PM EST

Labels: -merge-approved-88 merge-merged-4324 merge-merged-88

The following revision refers to this bug:

[https://chromium.googlesource.com/chromium/src/+db3b5f8d1cdfbc693827b05e341e1246fc88634a](https://chromium.googlesource.com/chromium/src/+/db3b5f8d1cdfbc693827b05e341e1246fc88634a)

commit [db3b5f8d1cdfbc693827b05e341e1246fc88634a](#)

Author: Sahel Sharify <[sahel@chromium.org](#)>

Date: Wed Feb 10 22:24:00 2021

[Merge to M88][Web Payment]PR_sheet_controller should not update views during PR abort

Similar to [crbug.com/903223](#)

PaymentRequestSheetController::UpdateHeaderView gets called after the payment request(PR) has been aborted. The fix for [crbug.com/903223](#) early returns in DidFinishNavigation which is the caller of UpdateHeaderView.

That's why calling UpdateHeaderView from a different function (e.g. DidChangeVisibleSecurityState in the case of [crbug.com/1165624](#)) still reproduces the issue.

This CL early returns in all PaymentRequestSheetController's Update...View functions when the PR is being aborted.

(cherry picked from commit [a1a3f9552ce156e3cc3bd0207e53b78609e4b07a](#))

[Bug: 1165624](#)

Change-Id: [Ie6f8f8ff6e72ef16878aa8dc3f15e19dea1587e1](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2635074>

Reviewed-by: Rouslan Solomakhin <[rouslan@chromium.org](#)>

Commit-Queue: Sahel Sharify <[sahel@chromium.org](#)>

Cr-Original-Commit-Position: refs/heads/master@{#844843}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2686273>

Cr-Commit-Position: refs/branch-heads/4324@{#2162}

Cr-Branched-From: [c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8](#)-refs/heads/master@{#827102}

[modify] https://crrev.com/db3b5f8d1cdfbc693827b05e341e1246fc88634a/chrome/browser/ui/views/payments/payment_request_sheet_controller.cc

[Comment 42](#) by [jorgelo@chromium.org](#) on Thu, Feb 11, 2021, 10:09 AM EST

Cc: [marinakz@chromium.org](#)

[Comment 43](#) by [amyressler@google.com](#) on Thu, Feb 11, 2021, 4:00 PM EST

Labels: -reward-unpaid reward-inprocess

[Comment 44](#) by [adetaylor@google.com](#) on Fri, Feb 12, 2021, 7:35 PM EST

Labels: Release-3-M88

[Comment 45](#) by [janag...@google.com](#) on Mon, Feb 15, 2021, 12:11 PM EST

Cc: [janag...@google.com](#)

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

[Comment 46](#) by [gianluca@google.com](#) on Tue, Feb 16, 2021, 3:44 AM EST

Labels: Merge-Approved-86-LTS

[Comment 47](#) by [bugdroid](#) on Tue, Feb 16, 2021, 1:14 PM EST

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+4c8fb4994cd1f2be91a3e0aee6fb5132f6ff5f36>

commit [4c8fb4994cd1f2be91a3e0aee6fb5132f6ff5f36](#)

Author: Sahel Sharify <[sahel@chromium.org](#)>

Date: Tue Feb 16 18:14:24 2021

[M86-LTS][Web Payment]PR_sheet_controller should not update views during PR abort

Similar to [crbug.com/903223](#)

PaymentRequestSheetController::UpdateHeaderView gets called after the payment request(PR) has been aborted. The fix for [crbug.com/903223](#) early returns in DidFinishNavigation which is the caller of UpdateHeaderView.

That's why calling UpdateHeaderView from a different function (e.g. DidChangeVisibleSecurityState in the case of [crbug.com/1165624](#)) still reproduces the issue.

This CL early returns in all PaymentRequestSheetController's Update...View functions when the PR is being aborted.

(cherry picked from commit [a1a3f9552ce156e3cc3bd0207e53b78609e4b07a](#))

[Bug: 1165624](#)

Change-Id: [Ie6f8f8ff6e72ef16878aa8dc3f15e19dea1587e1](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2635074>

Reviewed-by: Rouslan Solomakhin <[rouslan@chromium.org](#)>

Commit-Queue: Sahel Sharify <[sahel@chromium.org](#)>

Cr-Original-Commit-Position: refs/heads/master@{#844843}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2692922>

Reviewed-by: Victor-Gabriel Savu <[vsavu@google.com](#)>

Reviewed-by: Sahel Sharify <[sahel@chromium.org](#)>

Commit-Queue: Jana Grill <[janagrill@chromium.org](#)>

Cr-Commit-Position: refs/branch-heads/4240@{#1542}

Cr-Branched-From: f297677702651916bbf65e59c0d4bdd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/4c8fb4994cd1f2be91a3e0aee6fb5132f6ff5f36/chrome/browser/ui/views/payments/payment_request_sheet_controller.cc

Comment 48 by [janag...@google.com](#) on Wed, Feb 17, 2021, 5:08 AM EST

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

Comment 49 by [amyressler@google.com](#) on Mon, Feb 22, 2021, 4:31 PM EST

Labels: CVE-2021-21151 CVE_description-missing

Comment 50 by [amyressler@google.com](#) on Mon, Feb 22, 2021, 4:33 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 51 by [sheriffbot](#) on Tue, May 4, 2021, 1:50 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