



☆ Starred by 3 users

Owner:	<div> collinbaker@chromium.org</div> <div>Last visit 17 days ago</div>
CC:	<div> karandeepb@chromium.org</div> <div>pbos@chromium.org</div> <div>tbergquist@chromium.org</div> <div>connily@chromium.org</div> <div>dfried@chromium.org</div> <div>solomonkinard@chromium.org</div> <div>tjudkins@chromium.org</div>
Status:	Duplicate (Closed)
MergedInto:	issue-119362
Components:	Platform>Extensions>API
Modified:	Aug 19, 2021
Backlog-Rank:	---
Editors:	---
EstimatedDays:	---
NextAction:	---
OS:	Linux , Windows , Chrome , Mac , Lacros
Pri:	1
Type:	Bug-Security
<div>Hotlist-Merge-Review</div> <div>reward-10000</div> <div>Security_Impact-Stable</div> <div>Security_Severity-Medium</div> <div>allpublic</div> <div>reward-inprocess</div> <div>CVE_description-submitted</div> <div>M-91</div> <div>external_security_report</div> <div>CVE-2021-30520</div>	

Issue 1193362: Security: Heap-use-after-free in TabDragController::EndDragImpl

Reported by chrom...@gmail.com on Sun, Mar 28, 2021, 9:51 PM EDT

 Code

Chrome Version: 91.0.4461.0 (Official Build) canary (x86_64)
Operating System: MacOS

REPRODUCTION CASE

1. Install the extension.
2. Drag the opened tab out of the current tab strip

```
==14108==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e0009e8880 at pc 0x0001214dab15 bp 0x7fff5e855240 sp 0x7fff5e855238
READ of size 8 at 0x61e0009e8880 thread T0
#0 0x1214dab14 in TabDragController::EndDragImpl(TabDragController::EndDragType) tab_drag_controller.cc:769
#1 0x1214d1cb6 in TabDragController::EndDrag(EndDragReason) tab_drag_controller.cc:646
#2 0x1214d9335 in TabDragController::RunMoveLoop(gfx::Vector2d const&) tab_drag_controller.cc:1457
#3 0x1214de089 in TabDragController::DetachIntoNewBrowserAndRunMoveLoop(gfx::Point const&) tab_drag_controller.cc:1390
#4 0x1214dbcaf in TabDragController::DragBrowserToNewTabStrip(TabDragContext*, gfx::Point const&) tab_drag_controller.cc:865
#5 0x1214d9aeb in TabDragController::ContinueDragging(gfx::Point const&) tab_drag_controller.cc:831
#6 0x1214d2b13 in TabDragController::Drag(gfx::Point const&) tab_drag_controller.cc:604
#7 0x121533697 in TabStrip::TabDragContextImpl::ContinueDrag(views::View*, ui::LocatedEvent const&) tab_strip.cc:442
#8 0x12153fb4b in TabStrip::OnMouseDragged(ui::MouseEvent const&) tab_strip.cc:3666
#9 0x120108a3d in views::View::ProcessMouseDragged(ui::MouseEvent*) view.cc:2990
#10 0x118031b4f in ui::EventHandler::OnEvent(ui::Event*) event_handler.cc
#11 0x11802f39 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:191
#12 0x11802f714 in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) event_dispatcher.cc:84
#13 0x11802f450 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) event_dispatcher.cc:56
#14 0x12014075a in views::internal::RootView::OnMouseDragged(ui::MouseEvent const&) root_view.cc:457
#15 0x12015a697 in views::Widget::OnMouseEvent(ui::MouseEvent*) widget.cc:1335
#16 0x120196e6b in non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnMouseEvent(std::__1::unique_ptr<ui::Event, std::__1::default_delete<ui::Event> >)
native_widget_mac_ns_window_host.mm:804
#17 0x11c42d99b in-[BridgedContentView mouseEvent:] bridged_content_view.mm:586
#18 0x11c42ae7d in-[BridgedContentView processCapturedMouseEvent:] bridged_content_view.mm:308
#19 0x11c43891b in __ZN12remote_cocoa17CocoaMouseCapture14ActiveEventTap4InitEv_block_invoke mouse_capture.mm:91
#20 0x7fff92b357f9 in _NSSetSendEventToObservers+0x173 (AppKit:x86_64+0x1c77f9)
#21 0x7fff9312e23e in-[NSApplication(NSEvent) sendEvent:] +0x36 (AppKit:x86_64+0x7c023e)
#22 0x115c247d4 in __34-[BrowserCrApplication sendEvent:]_block_invoke chrome_browser_application_mac.mm:335
#23 0x114a5e299 in base::mac::CallWithEHFrame(void (*) block_pointer) +0x9 (Chromium Framework:x86_64+0xb8e299)
#24 0x115c23b4e in-[BrowserCrApplication sendEvent:] chrome_browser_application_mac.mm:319
#25 0x7fff929a93d6 in-[NSApplication run]+0x3e9 (AppKit:x86_64+0x3b3d6)
#26 0x114a726fa in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*) message_pump_mac.mm:691
#27 0x114a6e818 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*) message_pump_mac.mm:149
#28 0x114984a3b in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
thread_controller_with_message_pump_impl.cc:460
#29 0x1148c225e in base::RunLoop::Run(base::Location const&) run_loop.cc:133
#30 0x114f73823 in ChromeBrowserMainParts::MainMessageLoopRun(int*) chrome_browser_main.cc:1732
#31 0x10d5ca467 in content::BrowserMainLoop::RunMainMessageLoopParts() browser_main_loop.cc:970
#32 0x10d5ceb51 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:150
```

```
#33 0x10d5c39fc in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:47
#34 0x11469e7c4 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content_main_runner_impl.cc:581
#35 0x11469daf4 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:944
#36 0x11469ace6 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content_main.cc:372
#37 0x11469b2fc in content::ContentMain(content::ContentMainParams const&) content_main.cc:398
#38 0x108f7e1d5 in ChromeMain chrome_main.cc:141
#39 0x1013a940f in main chrome_exe_main_mac.cc:114
#40 0x7fffaab09234 in start+0x0 (libdyld.dylib:x86_64+0x5234)
```

0x61e0009e8880 is located 0 bytes inside of 2456-byte region [0x61e0009e8880,0x61e0009e9218)

freed by thread T0 here:

```
#0 0x1015a5fc9 (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x44fc9)
#1 0x115a3b882 in resource_coordinator::TabLifecycleUnitSource::TabLifecycleUnit::FinishDiscard(mojom::LifecycleUnitDiscardReason) memory:1335
#2 0x115a3bbf2 in resource_coordinator::TabLifecycleUnitSource::TabLifecycleUnit::Discard(mojom::LifecycleUnitDiscardReason) tab_lifecycle_unit.cc:566
#3 0x115a40511 in resource_coordinator::TabManager::DiscardTabByExtension(content::WebContents*) tab_manager.cc:239
#4 0x11f475dcc in extensions::TabsDiscardFunction::Run() tabs_api.cc:2399
#5 0x10f8b65b7 in ExtensionFunction::RunWithValidation() extension_function.cc:466
#6 0x10f8be7aa in extensions::ExtensionFunctionDispatcher::DispatchWithCallbackInternal(ExtensionHostMsg_Request_Params const&, content::RenderFrameHost*, int,
base::RepeatingCallback<void (ExtensionFunction::ResponseType, base::ListValue const&, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>
> const&)> const&) extension_function_dispatcher.cc:383
#7 0x10f8bd91a in extensions::ExtensionFunctionDispatcher::Dispatch(ExtensionHostMsg_Request_Params const&, content::RenderFrameHost*, int)
extension_function_dispatcher.cc:253
#8 0x10f932dd6 in extensions::ExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
extension_web_contents_observer.cc:327
#9 0x11f47e9f in extensions::ChromeExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
chrome_extension_web_contents_observer.cc:94
#10 0x10e6b7f72 in content::WebContentsImpl::OnMessageReceived(content::RenderFrameHostImpl*, IPC::Message const&) web_contents_impl.cc:1152
#11 0x10e1bc376 in content::RenderFrameHostImpl::OnMessageReceived(IPC::Message const&) render_frame_host_impl.cc:1940
#12 0x117f247f2 in IPC::ChannelProxy::Context::OnDispatchMessage(IPC::Message const&) ipc_channel_proxy.cc:325
#13 0x11494814f in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) callback.h:101
#14 0x11498381a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:351
#15 0x114983037 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:264
#16 0x114a70e03 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:358
#17 0x114a5e299 in base::mac::CallWithEHFrame(void (*) block_pointer)+0x9 (Chromium Framework:x86_64+0xbae8299)
#18 0x114a6f7d5 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:334
#19 0x7fff94ae0e50 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64+0xa4e50)
#20 0x7fff94ec20cb in __CFRunLoopDoSources0+0x22b (CoreFoundation:x86_64+0x860cb)
#21 0x7fff94ec15b5 in __CFRunLoopRun+0x3a5 (CoreFoundation:x86_64+0x855b5)
#22 0x7fff94ec0fb3 in CFRunLoopRunSpecific+0x1a3 (CoreFoundation:x86_64+0x84fb3)
#23 0x7fff9441febb in RunCurrentEventLoopInMode+0xef (HIToolbox:x86_64+0x30ebb)
#24 0x7fff9441fcd0 in ReceiveNextEventCommon+0x1af (HIToolbox:x86_64+0x30cf0)
#25 0x7fff9441fb25 in _BlockUntilNextEventMatchingListInModeWithFilter+0x46 (HIToolbox:x86_64+0x30b25)
#26 0x7fff929b4a03 in _DPSNextEvent+0x45f (AppKit:x86_64+0x46a03)
#27 0x7fff931307ed in -[NSApplication(NSEvent)_nextEventMatchingEventMask:untilDate:inMode:dequeue:]_+0xae (AppKit:x86_64+0x7c27ed)
#28 0x115c21dc2 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke chrome_browser_application_mac.mm:237
#29 0x114a5e299 in base::mac::CallWithEHFrame(void (*) block_pointer)+0x9 (Chromium Framework:x86_64+0xbae8299)
```

previously allocated by thread T0 here:

```
#0 0x1015a5e80 (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x44e80)
#1 0x1147c2067 in operator new(unsigned long) new.cpp:67
#2 0x10e6aaf4d in content::WebContentsImpl::CreateWithOpener(content::WebContents::CreateParams const&, content::RenderFrameHostImpl*)
web_contents_impl.cc:1008
#3 0x1207f12cf in Navigate(NavigateParams*) browser_navigator.cc:455
#4 0x11f5c4dfe in extensions::ExtensionTabUtil::OpenTab(ExtensionFunction*, extensions::ExtensionTabUtil::OpenTabParams const&, bool, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> >*) extension_tab_util.cc:313
#5 0x11462f3f in extensions::TabsCreateFunction::Run() tabs_api.cc:1170
#6 0x10f8b65b7 in ExtensionFunction::RunWithValidation() extension_function.cc:466
#7 0x10f8be7aa in extensions::ExtensionFunctionDispatcher::DispatchWithCallbackInternal(ExtensionHostMsg_Request_Params const&, content::RenderFrameHost*, int,
base::RepeatingCallback<void (ExtensionFunction::ResponseType, base::ListValue const&, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char>
> const&)> const&) extension_function_dispatcher.cc:383
#8 0x10f8bd91a in extensions::ExtensionFunctionDispatcher::Dispatch(ExtensionHostMsg_Request_Params const&, content::RenderFrameHost*, int)
extension_function_dispatcher.cc:253
#9 0x10f932dd6 in extensions::ExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
extension_web_contents_observer.cc:327
#10 0x11f47e9f in extensions::ChromeExtensionWebContentsObserver::OnMessageReceived(IPC::Message const&, content::RenderFrameHost*)
chrome_extension_web_contents_observer.cc:94
#11 0x10e6b7f72 in content::WebContentsImpl::OnMessageReceived(content::RenderFrameHostImpl*, IPC::Message const&) web_contents_impl.cc:1152
#12 0x10e1bc376 in content::RenderFrameHostImpl::OnMessageReceived(IPC::Message const&) render_frame_host_impl.cc:1940
#13 0x117f247f2 in IPC::ChannelProxy::Context::OnDispatchMessage(IPC::Message const&) ipc_channel_proxy.cc:325
#14 0x11494814f in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) callback.h:101
#15 0x11498381a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:351
#16 0x114983037 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:264
#17 0x114a70e03 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:358
#18 0x114a5e299 in base::mac::CallWithEHFrame(void (*) block_pointer)+0x9 (Chromium Framework:x86_64+0xbae8299)
#19 0x114a6f7d5 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:334
#20 0x7fff94ae0e50 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64+0xa4e50)
#21 0x7fff94ec20cb in __CFRunLoopDoSources0+0x22b (CoreFoundation:x86_64+0x860cb)
#22 0x7fff94ec15b5 in __CFRunLoopRun+0x3a5 (CoreFoundation:x86_64+0x855b5)
#23 0x7fff94ec0fb3 in CFRunLoopRunSpecific+0x1a3 (CoreFoundation:x86_64+0x84fb3)
#24 0x7fff9441febb in RunCurrentEventLoopInMode+0xef (HIToolbox:x86_64+0x30ebb)
#25 0x7fff9441fcd0 in ReceiveNextEventCommon+0x1af (HIToolbox:x86_64+0x30cf0)
#26 0x7fff9441fb25 in _BlockUntilNextEventMatchingListInModeWithFilter+0x46 (HIToolbox:x86_64+0x30b25)
#27 0x7fff929b4a03 in _DPSNextEvent+0x45f (AppKit:x86_64+0x46a03)
#28 0x7fff931307ed in -[NSApplication(NSEvent)_nextEventMatchingEventMask:untilDate:inMode:dequeue:]_+0xae (AppKit:x86_64+0x7c27ed)
#29 0x115c21dc2 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke chrome_browser_application_mac.mm:237
```

SUMMARY: AddressSanitizer: heap-use-after-free tab_drag_controller.cc:769 in TabDragController::EndDragImpl(TabDragController::EndDragType)

Shadow bytes around the buggy address:

```
0x1c3c0013d0c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d0d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d0e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d0f0: fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa
0x1c3c0013d100: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x1c3c0013d110:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d120: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d130: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d140: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d150: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x1c3c0013d160: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

Shadow byte legend (one shadow byte represents 8 application bytes):

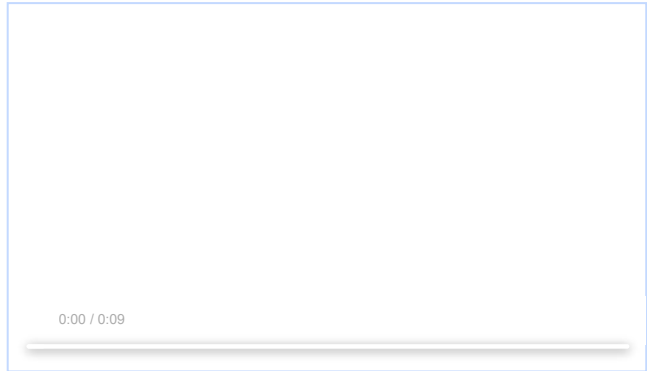
Addressable: 00

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

manifest.json
389 bytes [View](#) [Download](#)

background.js
219 bytes [View](#) [Download](#)

screen.mov
4.0 MB [View](#) [Download](#)



[Comment 1](#) by [sheriffbot](#) on Sun, Mar 28, 2021, 9:52 PM EDT Project Member
Labels: external_security_report

[Comment 2](#) by [kenrb@chromium.org](#) on Mon, Mar 29, 2021, 7:28 PM EDT Project Member
Status: Assigned (was: Unconfirmed)
Owner: tbergquist@chromium.org
Cc: dfried@chromium.org karandeepb@chromium.org connily@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium M-91 OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Platform>Extensions>API UI>Browser>TabStrip

Thanks for the report.

tbergquist@: Can you PTAL? This looks similar to [issue-4484054](#), but the trigger is different. This should be merged into that one if they have the same underlying cause.

These are significant security bugs. If you are unable to investigate then can you please help find another owner?

[Comment 3](#) by [sheriffbot](#) on Mon, Apr 12, 2021, 12:21 PM EDT Project Member
tbergquist: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

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

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

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

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

[Comment 4](#) by [connily@chromium.org](#) on Tue, Apr 13, 2021, 2:01 PM EDT Project Member
Owner: collinbaker@chromium.org
Cc: tbergquist@chromium.org

[Comment 5](#) by [collinbaker@chromium.org](#) on Thu, Apr 22, 2021, 6:27 PM EDT Project Member
Are you able to repro this on Linux? Assuming you have a Linux machine available.

I am not able to and I'm not sure if the bug is Mac only or if I'm not following the right steps.

[Comment 6](#) by [collinbaker@chromium.org](#) on Thu, Apr 22, 2021, 6:28 PM EDT Project Member
Cc: ppos@chromium.org

[Comment 7](#) by [chrom...@gmail.com](#) on Thu, Apr 22, 2021, 6:57 PM EDT
I am able to repro this on Linux.

[Comment 8](#) by [ppos@chromium.org](#) on Thu, Apr 22, 2021, 7:14 PM EDT Project Member
on Mac I get this as the top of the stack:

```
==67917==WARNING: Failed to use and restart external symbolizer!  
#0 0x12c43d92e in TabDragController::RestoreFocus()+0x12e (/Users/pos/chromium/src/out/asan/libchrome_dll.dylib:x86_64+0x151c792e)  
#1 0x12c43bd11 in TabDragController::EndDragImpl(TabDragController::EndDragType)+0x271  
(/Users/pos/chromium/src/out/asan/libchrome_dll.dylib:x86_64+0x151c5d11)
```

```
#2 0x12c42f9af in TabDragController::EndDrag(EndDragReason)+0x59f (/Users/pbos/chromium/src/out/asan/libchrome_dll.dylib:x86_64+0x151b99af)
#3 0x12c43a7b7 in TabDragController::RunMoveLoop(gfx::Vector2d const&)+0x1447 (/Users/pbos/chromium/src/out/asan/libchrome_dll.dylib:x86_64+0x151c47b7)
```

Comment 9 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:20 PM EDT Project Member

```
std::unique_ptr<content::WebContents> old_contents; deleter =
    tab_strip_model_>ReplaceWebContentsAt(index, std::move(null_contents));
```

Looks like after this call to ReplaceWebContentsAt does not invalidate the old referenced WebContents inside TabDragController and it's destroyed a few lines later.

https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/resource_coordinator/tab_lifecycle_unit.cc;l=538;drc=23fdafdac84e1a798865e4cc26f4f45e3152040c

Comment 10 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:40 PM EDT Project Member

It's possible that this got fixed in [r874810](#). If you sync does it still repro?

Comment 11 by [chrom...@gmail.com](#) on Thu, Apr 22, 2021, 7:48 PM EDT

I am not able to repro on Chromium 92.0.4486.0 refs/heads/master@(#875388). This seems like fixed in [r874810](#).

Comment 12 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:51 PM EDT Project Member

Status: Fixed (was: Assigned)

Thank you!

Comment 13 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:53 PM EDT Project Member

Looks like merging is being handled in [issue-1105573](#). I don't believe externally reported issues should be merged by me.

Comment 14 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:53 PM EDT Project Member

(externally reported security issues)

Comment 15 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 7:54 PM EDT Project Member

To whoever sees this, note that this bug is older than [issue-1105573](#).

Comment 16 by [chrom...@gmail.com](#) on Thu, Apr 22, 2021, 8:00 PM EDT

You're welcome!

So is this report qualified for a reward since this issue is older than [issue-1105573](#)?

Comment 17 by [pbos@chromium.org](#) on Thu, Apr 22, 2021, 8:07 PM EDT Project Member

It's not something handled by us directly so I can't say, I think they're automatically picked up by someone who'd be able to answer.

Comment 18 by [sheriffbot](#) on Fri, Apr 23, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 19 by [sheriffbot](#) on Fri, Apr 23, 2021, 1:55 PM EDT Project Member

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

Comment 20 by [sheriffbot](#) on Fri, Apr 23, 2021, 2:21 PM EDT Project Member

Labels: Merge-Request-91

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M91. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

Comment 21 by [sheriffbot](#) on Fri, Apr 23, 2021, 2:23 PM EDT Project Member

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), bindusuvama@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 22 by [pbos@chromium.org](#) on Fri, Apr 23, 2021, 2:30 PM EDT Project Member

Merging is covered in [issue-1105573](#).

Comment 23 by [amyressler@chromium.org](#) on Fri, Apr 23, 2021, 4:02 PM EDT Project Member

Status: Duplicate (was: Fixed)

Mergedinto: 1195573

Comment 24 by [amyressler@chromium.org](#) on Fri, Apr 23, 2021, 4:04 PM EDT Project Member

Merging this as a duplicate as the fix was landed in the other bug. We do note and are aware that 1195573 is the later reported issue.

So Khalil, don't worry - we are aware and have noted that yours is the earlier reported bug, so it will go to the VRP Panel and you'll be rewarded and credited for it. :)

Comment 25 by [sheriffbot](#) on Sat, Apr 24, 2021, 12:36 PM EDT Project Member

Labels: -reward-topanel reward-ineligible

Comment 26 by [adetaylor@google.com](#) on Mon, Apr 26, 2021, 6:41 PM EDT Project Member

Labels: -Merge-Review-91

Comment 27 by amyressler@chromium.org on Wed, Apr 28, 2021, 7:49 PM EDT Project Member

Labels: -reward-ineligible reward-topanel

Comment 28 by amyressler@google.com on Wed, Apr 28, 2021, 7:49 PM EDT Project Member

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

*** Boilerplate reminders! ***

Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.

Comment 29 by amyressler@chromium.org on Wed, Apr 28, 2021, 7:50 PM EDT Project Member

Congratulations, Khalil! The VRP Panel has decided to award you \$10,000 for this report. Nice finding!

Comment 30 by amyressler@google.com on Fri, Apr 30, 2021, 1:56 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 31 by amyressler@google.com on Mon, May 10, 2021, 9:55 AM EDT Project Member

Labels: CVE-2021-30520 CVE_description-missing

Comment 32 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 33 by sheriffbot on Thu, Aug 19, 2021, 1:30 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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