☆ Starred by 1 user

Owner:	a...@chromium.org
CC:	csharrison@chromium.org robliao@chromium.org mustaq@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>FullScreen
Modified:	Jun 20, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
M-80
allpublic
reward-inprocess
CVE_description-submitted
Release-0-M83
CVE-2020-6475

Issue 1020026: Security: 'Press Esc to exit fullscreen' covered up by a popup page

Reported by chrom...@gmail.com on Wed, Oct 30, 2019, 10:02 PM EDT

Code

VERSION
Chrome Version: 80.0.3953.5 Canary
Operating System: Windows

This is the same as ~~issue 882363~~.

REPRODUCTION CASE
1. Go to http://1vpctucm.3cm.me/fullscreen.html
2. Switch http://1vpctucm.3cm.me/fullscreen.html page
3. Switch the popup page and click on any key

* The "Press esc" message is covered up by a popup page.

Note: I wasn't able to repro this on macOS.

fullscreen.html
427 bytes View Download

fullscreen2.html
507 bytes View Download

Comment 1 by chrom...@gmail.com on Wed, Oct 30, 2019, 10:07 PM EDT

screen.mov
2.3 MB View Download

Comment 2 by livvielin@chromium.org on Thu, Oct 31, 2019, 2:39 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: a...@chromium.org
Labels: Security_Impact-Head Security_Severity-Medium M-80 OS-Windows Pri-1
Components: UI>Browser>FullScreen

Adding avi, who handled ~~issue 882363~~. Would you be able to help take a look, or pass off to someone else if needed? Thanks!

Comment 3 by a...@chromium.org on Thu, Oct 31, 2019, 2:55 PM EDT Project Member

Cc: csharrison@chromium.org

I'm digging.

OP: Your video has the original page maximized, which makes the effect unclear. In the future, please start with a non-maximized window so that it's clear what the effect is.

Meanwhile, from the source I see:

- Page 1 opens page 2 as a popup.
- Page 2, on user gesture, causes page 1 to go fullscreen, then opens a new blank popup, and then attempts to close *something*

Comment 4 by a...@chromium.org on Thu, Oct 31, 2019, 3:02 PM EDT Project Member

Cc: mustaq@chromium.org

Note that the initial popup from page 1 is blocked by a popup blocker but that's easily worked around.

I can't get this to work in 78.0.3904.70. On page 2, if I press a key I get the second blank popup, but nothing goes fullscreen and nothing closes. In the console of page 1 I see:

fullscreen2.html:10 Failed to execute 'requestFullscreen' on 'Element': API can only be initiated by a user gesture.

The failure to close doesn't surprise me; we very heavily restrict the ability of pages to close each other. Mustaq, has anything changed with regard to user gestures lately?

Comment 5 by mustaq@chromium.org on Thu, Oct 31, 2019, 3:21 PM EDT Project Member

The last change I can recall is fullscreen request consuming user activation (https://www.chromestatus.com/feature/5156313334022144) on M76. We landed some cleanup CLs recently but those should affect only pre-UAv2 behavior.

Comment 6 by a...@chromium.org on Thu, Oct 31, 2019, 3:40 PM EDT Project Member

OP, in your video, at about 4.5 seconds in, you're manually switching windows, which isn't accounted for in your repro steps.

You use the word "switch" several times. Can you clarify exactly what you mean by that? When do you click on the pages, when do you press a button on the keyboard, when do you manually switch pages?

Comment 7 by a...@chromium.org on Thu, Oct 31, 2019, 3:45 PM EDT Project Member

Here's the repro I'm somewhat able to get:

1. Open http://1vpctucm.3cm.me/fullscreen.html. (It will open a popup.)
2. Click on that page. Click around to make sure it has a user activation.
3. Switch back to the popup.
4. Press a key.

On the Mac, I'm seeing that the page does go fullscreen, but immediately loses it when the second popup is opened. I'm going to see how that works on Windows now. OP, is that the behavior you see on Windows?

Comment 8 by chrom...@gmail.com on Thu, Oct 31, 2019, 4:26 PM EDT

Comment#7 > Yes exactly.

On the Windows the page stays in full-screen mode even when the second popup is opened, not like on the Mac.

Comment 9 by chrom...@gmail.com on Thu, Oct 31, 2019, 4:28 PM EDT

screen2.mp4
234 KB View Download

Comment 10 by sheriffbot@chromium.org on Fri, Nov 1, 2019, 9:56 AM EDT Project Member

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

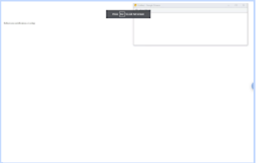
Comment 11 by a...@chromium.org on Fri, Nov 1, 2019, 2:13 PM EDT Project Member

Cc: robliao@chromium.org

I'm seeing the bubble overlap both windows.

Rob: You know Windows and Views. Are there scenarios where the fullscreen bubble would be below the windows here?

Screen Shot 2019-11-01 at 2.10.58 PM.png
152 KB View Download



Comment 12 by a...@chromium.org on Fri, Nov 1, 2019, 2:13 PM EDT Project Member

(And it's still not clear to me why the popup doesn't cause the fullscreen to be lost.)

Comment 13 by robliao@chromium.org on Fri, Nov 1, 2019, 2:46 PM EDT Project Member

Looking at the code (don't have easy access to a windows machine at the moment), it's possible.

https://cs.chromium.org/chromium/src/chrome/browser/ui/views/exclusive_access_bubble_views.cc?rcl=1e8d3cf5b753ad433f7d7f03a8984a43a964a4ed&l=79

Sets up the widget to display the bubble a la a SubtleNotificationView, but SubtleNotificationView does not know that ExclusiveAccessBubbleViews wants a non-normal ZOrder at Widget init time. This means that the code to set WS_EX_TOPMOST doesn't get run.

https://cs.chromium.org/chromium/src/ui/views/widget/widget_hwnd_utils.cc?rcl=75fb429759aa71bae59cdd57b69a482c1153579e&l=49

Later on, when ExclusiveAccessBubbleViews does this...
popup_->SetZOrderLevel(ui::ZOrderLevel::kSecuritySurface);
It's too late and that doesn't get forwarded to Windows by Aura.

I can take a closer look at this path if need be.

However I do agree that creating a popup should likely dismiss fullscreen mode.

Comment 14 by a...@chromium.org on Fri, Nov 1, 2019, 3:01 PM EDT Project Member

The code to dismiss fullscreen when a popup is created was put into Chrome years ago. The question that I have is why it's not working on Windows when it's working correctly on the Mac and Linux.

Comment 15 by robliao@chromium.org on Fri, Nov 1, 2019, 3:04 PM EDT Project Member

Sounds like we need a bisect here. Can we require that for these sorts of bugs?

Comment 16 by a...@chromium.org on Fri, Nov 1, 2019, 3:07 PM EDT Project Member

Assuming it ever worked in the first place. I don't kick out *every* fullscreen page when a popup happens, only when they're related. And the fact that it happens on the Mac means that it's likely some cross-platform weirdity.

Comment 17 by sheriffbot@chromium.org on Sat, Nov 16, 2019, 9:11 AM EST Project Member

avi: 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 18 by sheriffbot@chromium.org on Sun, Dec 1, 2019, 9:10 AM EST Project Member avi: Uh oh! This issue still open and hasn't been updated in the last 29 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 19 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:11 AM EST Project Member
Labels: -Security_Impact-Head Security_Impact-Beta

Comment 20 by srinivassista@google.com on Mon, Jan 6, 2020, 4:19 PM EST Project Member
This bug is marked as stable blocker for M80. Please review the bug and if it should not block stable release, please remove the RBS label. If it is indeed a stable blocker, pls help get a fix landed and ready to merge to M80 so it can be baked in the beta channel

Comment 21 by srinivassista@google.com on Thu, Jan 9, 2020, 1:16 AM EST Project Member
avi@ friendly ping to help look into this RBS for M80 ^

Comment 22 by srinivassista@google.com on Fri, Jan 10, 2020, 6:47 PM EST Project Member
friendly ping ^

Comment 23 by a...@chromium.org on Thu, Jan 16, 2020, 2:27 PM EST Project Member
Labels: -ReleaseBlock-Stable

Investigating, but I don't see this as RBS.

Comment 24 by adetaylor@google.com on Thu, Jan 16, 2020, 2:42 PM EST Project Member
Labels: -Security_Impact-Beta Security_Impact-Stable

Setting security impact to stable per #c23 (otherwise Sheriffbot will add RBS back again). avi@, if you determine that this bug doesn't affect stable please reset Security_Impact as appropriate, so it goes through the right merge processes, release notes, VRP etc.

Comment 25 by bugdroid on Fri, Mar 6, 2020, 4:33 PM EST Project Member
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/d1d25656154f09c4c7a689aaa2df0044d5e02f93

commit d1d25656154f09c4c7a689aaa2df0044d5e02f93
Author: Avi Drissman <avi@chromium.org>
Date: Fri Mar 06 21:28:58 2020

Prevent fullscreen while dialogs are up (1/2)

Chromium already drops fullscreen when a dialog is first displayed.
Extend that behavior so that a WebContents may not enter fullscreen
for the duration of a dialog's display.

This is part 1: Extend the fullscreen IPC so that the browser can
decline a renderer's request to enter fullscreen.

~~Bug: 1042210~~, ~~1020026~~, ~~1037730~~
Change-Id: Iafba087b22c51bf3c8fb6f9a4ce02921d51f0044
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2041871
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Reviewed-by: Philip Jägenstedt <foolip@chromium.org>
Reviewed-by: Dave Tapuska <dtapuska@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/master@{#747870}

[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/frame_host/render_frame_host_delegate.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/frame_host/render_frame_host_delegate.h
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/frame_host/render_frame_host_impl.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/frame_host/render_frame_host_impl.h
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/screen_orientation/screen_orientation_provider_unittest.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/public/mojom/frame/frame.mojom
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/frame/fullscreen_controller.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/frame/fullscreen_controller.h
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/fullscreen/fullscreen.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/fullscreen/fullscreen.h
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/html/media/html_media_element_event_listeners_test.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/html/media/html_video_element_persistent_test.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/html/media/video_auto_fullscreen_test.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/testing/fake_local_frame_host.cc
[modify] https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/core/testing/fake_local_frame_host.h
[modify]
https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/modules/media_controls/elements/media_control_display_cutout_fullscreen_button_element_test.cc
[modify]
https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/modules/media_controls/media_controls_display_cutout_delegate_test.cc
[modify]
https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/modules/media_controls/media_controls_orientation_lock_delegate_test.cc
[modify]
https://crrev.com/d1d25656154f09c4c7a689aaa2df0044d5e02f93/third_party/blink/renderer/modules/media_controls/media_controls_rotate_to_fullscreen_delegate_test.cc

Comment 26 by bugdroid on Tue, Mar 10, 2020, 3:01 PM EDT Project Member
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee

commit 1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee
Author: Avi Drissman <avi@chromium.org>
Date: Tue Mar 10 18:56:45 2020

Prevent fullscreen while dialogs are up (2/2)

Chromium already drops fullscreen when a dialog is first displayed.

Extend that behavior so that a WebContents may not enter fullscreen
for the duration of a dialog's display.

This is part 2: Modify WebContents::ForSecurityDropFullscreen() to
support a span of time that fullscreen is prohibited and modify all
callers to correctly request that span.

~~Bug: 1042210~~, ~~1020026~~, ~~1037730~~
Change-Id: I9d2ccc1e459cf37bfbf3499063d87d93ef9910e8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2044658
Commit-Queue: Avi Drissman <avi@chromium.org>
Reviewed-by: Balazs Engedy <engedy@chromium.org>
Reviewed-by: Christopher Thompson <cthomp@chromium.org>
Reviewed-by: Victor Costan <pwnall@chromium.org>
Cr-Commit-Position: refs/heads/master@{#748808}

[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/custom_handlers/register_protocol_handler_permission_request.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/custom_handlers/register_protocol_handler_permission_request.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/native_file_system/chrome_native_file_system_permission_context.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/native_file_system/native_file_system_permission_request_manager.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/native_file_system/native_file_system_permission_request_manager.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/native_file_system/origin_scoped_native_file_system_permission_context.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/native_file_system/tab_scoped_native_file_system_permission_context.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/permissions/permission_request_manager_browsertest.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/browser.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/native_file_system_dialogs.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/native_file_system_dialogs.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/views/native_file_system/native_file_system_directory_access_confirmation_view.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/views/native_file_system/native_file_system_directory_access_confirmation_view.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/chrome/browser/ui/views/native_file_system/native_file_system_directory_access_confirmation_view_browsertest.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/BUILD.gn
[add] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/frame_host/file_chooser_impl.cc
[add] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/frame_host/file_chooser_impl.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/frame_host/render_frame_host_delegate.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/frame_host/render_frame_host_delegate.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/frame_host/render_frame_host_impl.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/native_file_system/file_system_chooser.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/native_file_system/file_system_chooser.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/native_file_system/file_system_chooser_unittest.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/native_file_system/native_file_system_manager_impl.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/browser/web_contents/web_contents_impl_browsertest.cc
[modify] https://crrev.com/1a55a9d654522ebc4d54baa0aa0b8a9697e3c1ee/content/public/browser/web_contents.h

Comment 27 by a...@chromium.org on Tue, Mar 10, 2020, 3:06 PM EDT Project Member

I believe these changes should fix this. PTAL and let me know.

Comment 28 by chrom...@gmail.com on Wed, Mar 11, 2020, 9:05 AM EDT

Unable to repro this on 82.0.4083.0 canary on Windows 7. Fixed.

Comment 29 by a...@chromium.org on Wed, Mar 11, 2020, 1:50 PM EDT Project Member

Status: Fixed (was: Assigned)

Whoo!!!!

Comment 30 by sheriffbot on Wed, Mar 11, 2020, 2:05 PM EDT Project Member

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

Comment 31 by natashapabrai@google.com on Mon, Mar 16, 2020, 6:43 PM EDT Project Member

Labels: reward-topanel

Comment 32 by sheriffbot on Tue, Mar 17, 2020, 2:26 PM EDT Project Member

Labels: Merge-Request-81

Requesting merge to beta M81 because latest trunk commit (748808) appears to be after beta branch point (737173).

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

Comment 33 by sheriffbot on Tue, Mar 17, 2020, 2:28 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: Request affecting a post-stable build
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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

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

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

Comment 34 by a...@chromium.org on Tue, Mar 17, 2020, 9:13 PM EDT Project Member

Labels: -Merge-Review-81

nononono. This is a super complicated patch. I don't feel safe merging it. Sorry, sheriffbot.

Comment 35 by natashapabrai@google.com on Thu, Mar 19, 2020, 12:08 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 36 by natashapabrai@google.com on Thu, Mar 19, 2020, 12:14 PM EDT Project Member

Congrats! The Panel decided to award $1,000 for this report!

Comment 37 by natashapabrai@google.com on Thu, Mar 26, 2020, 5:58 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 38 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 39 by adetaylor@chromium.org on Mon, May 18, 2020, 11:58 AM EDT Project Member

Labels: CVE-2020-6475 CVE_description-missing

Comment 40 by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 41 by sheriffbot on Sat, Jun 20, 2020, 2:58 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