☆ Starred by 3 users

Owner:	ellyj...@chromium.org
CC:	adetaylor@chromium.org elainechien@chromium.org wry@chromium.org victorvianna@google.com mac-bugs-priority@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Sharing
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Mac
Pri:	1
Type:	Bug-Security

reward-5000
Needs-TestConfirmation
Needs-Feedback
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
FoundIn-100
Security_Impact-Extended
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1481

Issue 1302949: Security: Heap-use-after-free in send_tab_to_self::SendTabToSelfBubbleController::OnBubbleClosed

Reported by merc....@gmail.com on Fri, Mar 4, 2022, 6:41 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.109 Safari/537.36

Steps to reproduce the problem:

1. download asan-mac-release-975711.zip and unzip
2. start a server at poc.html: python -m SimpleHTTPServer 8605
3. ./Chromium --user-data-dir=/path/to/your/chrome/user-data-dir http://127.0.0.1:8605/poc.html
   Please use a user-data-dir that have login the google account, and have the menu `send to your devices`
4. After open chromium, open `send to your devices` twice, and you will get two bubble shown at the same time
5. wait until crash.

What is the expected behavior?

What went wrong?
It seems that the window of `send to your devices` not disappeared after click. So we can get more than one bubble at one time.

Did this work before? N/A

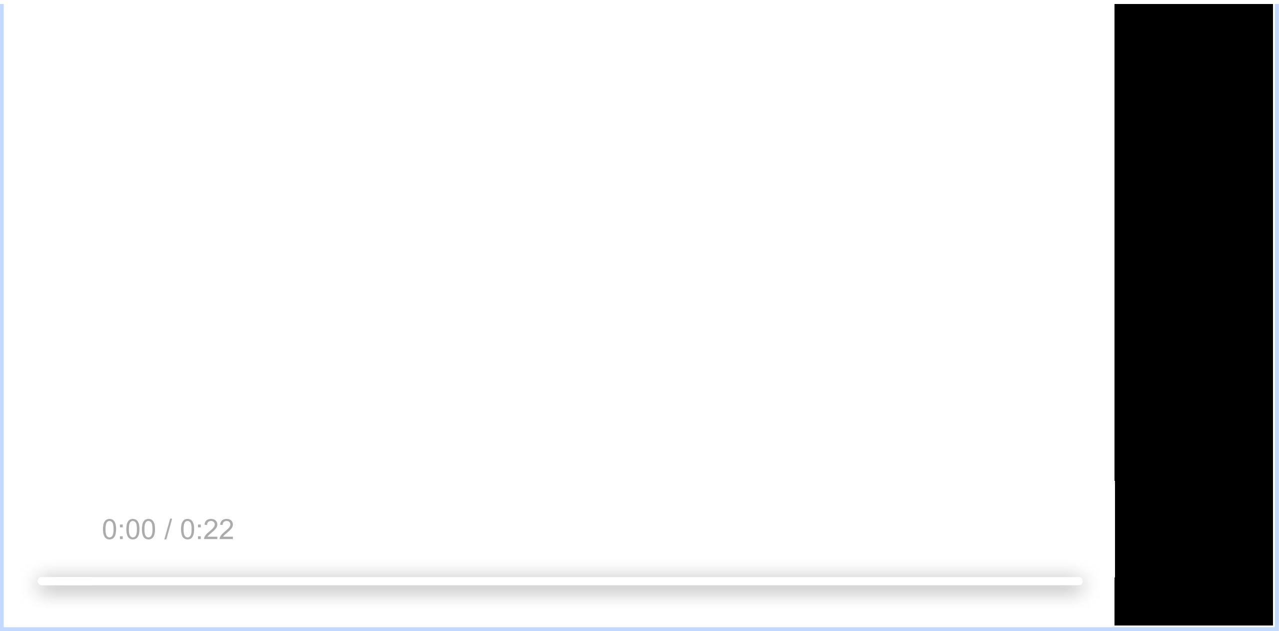
Chrome version: 98.0.4758.109 Channel: n/a
OS Version: OS X 10.15.7

poc.html
173 bytes View Download

asan.txt
23.1 KB View Download

video.mov
5.8 MB View Download

[redacted]



Comment 1 by sheriffbot on Fri, Mar 4, 2022, 6:45 AM EST Project Member

Labels: external_security_report

Comment 2 by dcheng@chromium.org on Tue, Mar 8, 2022, 6:04 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: markeh@google.com
Components: UI>Browser>Sharing

I wonder if this is Mac-specific? I don't have a Mac available to test, but at least on CrOS, the Send To Your Devices bubble disappears as soon as I right-click again, so I cannot reproduce this.

Assigning a random owner from //chrome/browser/share/OWNERS who might be able to take a closer look; even if this ends up being a low-severity security issue, it seems like it'd be good to fix if it can be reproduced.

Comment 3 by merc....@gmail.com on Tue, Mar 8, 2022, 6:09 AM EST

Yes, I can only trigger this on Mac.BTW, I use Mac with M1 chip.

Comment 4 by markeh@google.com on Wed, Mar 9, 2022, 7:31 PM EST Project Member

Owner: wry@chromium.org

Comment 5 by wry@chromium.org on Wed, Mar 9, 2022, 7:37 PM EST Project Member

Unfortunately I'm not able to reproduce this issue on my intel mac running 12.2.1. (the bubble disappears as soon as I right-click again, similar to the behavior mentioned in Comment 2) even for the specific Chrome version listed.

Tomorrow I will ask around about the tools available for repro on specific OS versions and/or hardware.

Out of curiosity, does this issue occur for you on any webpage or only for the one provided? (I did try to reproduce with the exact steps listed fwiw)

Comment 6 by merc....@gmail.com on Wed, Mar 9, 2022, 8:40 PM EST

It occurs on any webpages.

Comment 7 by wry@chromium.org on Thu, Mar 10, 2022, 12:39 PM EST Project Member

Labels: Needs-TestConfirmation

Comment 8 by adetaylor@google.com on Thu, Mar 17, 2022, 12:23 PM EDT Project Member

Status: WontFix (was: Assigned)
Cc: adetaylor@chromium.org

Tried to reproduce with asan-mac-release-950343 and also asan-mac-release-975711. Unfortunately I also can't reproduce it. Like in #c5 I see the bubble disappear immediately as soon as I do the second right-click. (I too am using a more modern OS X version).

As three of us have tried to reproduce this, I don't think this is actionable and I'm afraid I'm going to have to mark this as WontFix. merc.ouc@ we would like to fix this: if you can provide any more help in getting us to reproduce it, I'll be happy to reopen it.

A few things...
1) please could you confirm your MacOS version? You say 10.15.7 and yet you say you're using an M1 Mac. I thought M1 was supported only from OS X 11 onwards. In any case, it would be great if you can confirm this reproduces on OS X 12.2.1 since that's what we're all using. If you determine that this is specific to older OS versions then that would at least help us understand why none of us can reproduce this.

2) the asan.txt in #c0 suggests that there is some page close event taking place? (From the 'free' stack). I can't see that in your video. You didn't happen to do Cmd-W or anything to close the tab?

3) Please also re-confirm that you saw this on 975711. There have been multiple UaF fixes in this code recently, so the precise version might actually matter down to just a few revisions. It's quite likely that this may turn out to be a duplicate, though I couldn't see an exactly matching issue.

Sorry to have to close this down as non-actionable. We have no doubt that there's a real bug here, but we can't do anything to fix it right now. Again I'll be happy to reopen it if you can provide additional information that helps get us to a point where we can reproduce this. Thanks.

Comment 9 by merc....@gmail.com on Thu, Mar 17, 2022, 9:54 PM EDT

Actually the page close event happened in the poc.html : 'window.close();'.
And I found a similar patch for QR code generator, maybe it can help you to patch this one: https://chromium-review.googlesource.com/c/chromium/src/+/3489106

Comment 10 by merc....@gmail.com on Tue, Mar 22, 2022, 10:21 PM EDT

any updates?

Comment 11 by adetaylor@chromium.org on Thu, Mar 24, 2022, 10:38 AM EDT Project Member

Ah yes I didn't spot the window.close() in the POC, thanks.

Please could you answer questions 1 and 3.

Comment 12 by merc....@gmail.com on Thu, Mar 24, 2022, 9:53 PM EDT

Sorry, my MacOS's version is 12.2.1
I have confirmed that this bug is still reproducible in `asan-mac-release-984129` with this version: `102.0.4959.0`
Hope this can help you

Hope this can help you.

Comment 13 by adetaylor@chromium.org on Thu, Mar 24, 2022, 9:54 PM EDT Project Member

Status: Unconfirmed (was: WontFix)

Thanks, reopening so we take a look with this new information.

Comment 14 by sheriffbot on Sun, Mar 27, 2022, 2:27 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 15 by adetaylor@google.com on Mon, Apr 4, 2022, 6:15 PM EDT Project Member

I still can't reproduce this with asan-mac-release-984129.

I also still don't understand how the window is closing and resulting in profile destruction.

I feel you must have slight differences between:
- the poc
- the scenario in the video
- the asan trace.

Scripts can't close their own window, so the window.close() in the poc doesn't work. Developer tools says:
> poc.html:5 Scripts may close only the windows that were opened by them. (anonymous) @ poc.html:5
as I'd expect.

So unless you're doing ⌘-W to close the window at some point, I don't understand how you're getting the ASAN trace that you're seeing.

Please could you check everything you uploaded is 100% matching?

The symptoms I see are also a little different from your view. As soon as I open the second pop-up menu, the "share with devices" pop-up window disappears.

Comment 16 by danakj@chromium.org on Tue, Apr 5, 2022, 11:22 AM EDT Project Member

Labels: Needs-Feedback

Comment 17 by merc....@gmail.com on Tue, Apr 5, 2022, 10:32 PM EDT

If the scripts can't close the window, you can close it by click or commadn+W, it doesn't impact the bug.
I'm pretty sure the attachment is matching, I don't figure out why the old popup didn't disappear, but it actually happened.

Comment 18 by adetaylor@google.com on Thu, Apr 7, 2022, 12:56 PM EDT Project Member

Owner: ellyj...@chromium.org
Cc: wry@chromium.org
Labels: Security_Severity-High FoundIn-100 Pri-1

I did also try manually closing the window in various ways; I can't reproduce this bug.

As security sheriffs, we try to give a clear reproducible case over to engineering, and in this case we're failing. Of course, I think it's likely that there is a real bug here, but it may not be actionable.

So: I'm going to formally pass this to engineering in the hopes that there is enough information in the ASAN trace. But wry/others@, if you can't make any progress, please close this as WontFix. We do not want un-actionable security bugs wry/others@, if you can't make any progress, please close this as WontFix. We do not want un-actionable security bugs hanging around.

As a browser process UaF this would be Critical severity, but it seems clear that it involves some destruction and/or some UI interaction, so that mitigates it down to High. I'm going to assume this has existed since M100 or earlier and label up thus.

wry@ appears to be long-term OOO so Elly, could you figure out a good owner here?

Comment 19 by sheriffbot on Thu, Apr 7, 2022, 1:12 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 20 by ellyj...@chromium.org on Fri, Apr 8, 2022, 11:57 AM EDT Project Member

Hmmm.

Well, SendTabToSelfBubbleController and SendTabToSelfBubbleViewImpl hold raw pointers to each other but their lifetimes aren't coupled, which certainly seems Hella Sketch even if we can't figure out how to make this bug actually reproduce. The general pattern of having a controller which is a WebContentsUserData (i.e. owned by WebContents) and a View that has a raw pointer to that controller is inherently prone to this type of bug.

I'll swap the raw View -> Controller pointer out for a WeakPtr, which should mitigate this issue. Speculative fix ahoy!

Comment 21 by Git Watcher on Fri, Apr 8, 2022, 1:11 PM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/88d48019fa49b27478269aeff2068223b35b1e5d

commit 88d48019fa49b27478269aeff2068223b35b1e5d
Author: Elly Fong-Jones <ellyjones@chromium.org>
Date: Fri Apr 08 17:10:31 2022

stts: don't hold raw view->controller pointer

The general pattern of:
1. A controller which is owned by a WebContents via WebContentsUserData
2. A view (which is owned by Views) holding a raw pointer to that
   controller

is inherently prone to lifetime bugs at window closure, because window closure happens asynchronously but the WebContents teardown (& controller deallocation) happen synchronously, meaning the View teardown path (which often calls back into the controller) happens on a now-dead controller. Using a WeakPtr to reference the controller from the View avoids this problem.

~~Fixed: 1302949~~
Change-Id: I764a4053c2f02d277fcb275854351f77430cfb68
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3577583
Reviewed-by: Travis Skare <skare@chromium.org>

Commit-Queue: Elly Fong-Jones <ellyjones@chromium.org>
Cr-Commit-Position: refs/heads/main@{#990456}

[modify]
https://crrev.com/88d48019fa49b27478269aeff2068223b35b1e5d/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.cc
[modify]
https://crrev.com/88d48019fa49b27478269aeff2068223b35b1e5d/chrome/browser/ui/send_tab_to_self/send_tab_to_self_bubble_controller.h
[modify]
https://crrev.com/88d48019fa49b27478269aeff2068223b35b1e5d/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.h

Comment 22 by sheriffbot on Sat, Apr 9, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 23 by sheriffbot on Sat, Apr 9, 2022, 1:40 PM EDT Project Member

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

Comment 24 by amyressler@chromium.org on Tue, Apr 12, 2022, 9:53 PM EDT Project Member

Labels: Merge-Review-100 Merge-Review-101

investigating why sheriffbot isn't setting merge triage labels on certain security bugs, adding manual in the meantime to mind the gap

Comment 25 by amyressler@google.com on Wed, Apr 13, 2022, 7:42 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 26 by amyressler@chromium.org on Wed, Apr 13, 2022, 7:51 PM EDT Project Member

Thank you for this report. The VRP Panel has decided to award you $5,000 due to the moderate user interaction required and that this issue appears to be somewhat mitigated from being effectively triggered. Thank you for your efforts and reporting this issue to us.

Comment 27 by amyressler@chromium.org on Fri, Apr 15, 2022, 7:59 PM EDT Project Member

Labels: -Merge-Review-100 -Merge-Review-101 Merge-Approved-101 Merge-Approved-100

hi elly, thanks for the speculative fix for this difficult to reproduce issue! m101 and m100 merges approved, please merge this fix (before noon PST, Tuesday, 19 April) to branches 4951 and 4896 respectively so this fix can be included in the stable and extended stable cuts of M101 and M100.

Comment 28 by amyressler@google.com on Fri, Apr 15, 2022, 10:00 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 29 by Git Watcher on Tue, Apr 19, 2022, 12:10 PM EDT Project Member

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/04091a4a6e8f4f35a1daa2d6a02e51a3ec28dd8f

commit 04091a4a6e8f4f35a1daa2d6a02e51a3ec28dd8f
Author: Elly Fong-Jones <ellyjones@chromium.org>
Date: Tue Apr 19 16:09:19 2022

[M101] stts: don't hold raw view->controller pointer

The general pattern of:
1. A controller which is owned by a WebContents via WebContentsUserData
2. A view (which is owned by Views) holding a raw pointer to that
controller

is inherently prone to lifetime bugs at window closure, because window
closure happens asynchronously but the WebContents teardown (&
controller deallocation) happen synchronously, meaning the View teardown
path (which often calls back into the controller) happens on a now-dead
controller. Using a WeakPtr to reference the controller from the View
avoids this problem.

(cherry picked from commit 88d48019fa49b27478269aeff2068223b35b1e5d)

~~Fixed: 1302949~~
Change-Id: I764a4053c2f02d277fcb275854351f77430cfb68
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3577583
Reviewed-by: Travis Skare <skare@chromium.org>
Commit-Queue: Elly Fong-Jones <ellyjones@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#990456}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3594279
Auto-Submit: Elly Fong-Jones <ellyjones@chromium.org>
Commit-Queue: Travis Skare <skare@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#886}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/04091a4a6e8f4f35a1daa2d6a02e51a3ec28dd8f/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.cc
[modify]
https://crrev.com/04091a4a6e8f4f35a1daa2d6a02e51a3ec28dd8f/chrome/browser/ui/send_tab_to_self/send_tab_to_self_bubble_controller.h
[modify]
https://crrev.com/04091a4a6e8f4f35a1daa2d6a02e51a3ec28dd8f/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.h

Comment 30 by Git Watcher on Tue, Apr 19, 2022, 12:16 PM EDT Project Member

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:

https://chromium.googlesource.com/chromium/src/+/75362bbcdb231fd33c93f95c22edebe571122c61

commit 75362bbcdb231fd33c93f95c22edebe571122c61
Author: Elly Fong-Jones <ellyjones@chromium.org>
Date: Tue Apr 19 16:15:52 2022

[M100] stts: don't hold raw view->controller pointer

The general pattern of:
1. A controller which is owned by a WebContents via WebContentsUserData
2. A view (which is owned by Views) holding a raw pointer to that
   controller

is inherently prone to lifetime bugs at window closure, because window
closure happens asynchronously but the WebContents teardown (&
controller deallocation) happen synchronously, meaning the View teardown
path (which often calls back into the controller) happens on a now-dead
controller. Using a WeakPtr to reference the controller from the View
avoids this problem.

(cherry picked from commit 88d48019fa49b27478269aeff2068223b35b1e5d)

~~Fixed: 1302949~~
Change-Id: I764a4053c2f02d277fcb275854351f77430cfb68
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3577583
Reviewed-by: Travis Skare <skare@chromium.org>
Commit-Queue: Elly Fong-Jones <ellyjones@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#990456}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3594280
Auto-Submit: Elly Fong-Jones <ellyjones@chromium.org>
Commit-Queue: Travis Skare <skare@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#1153}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/75362bbcdb231fd33c93f95c22edebe571122c61/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.cc
[modify]
https://crrev.com/75362bbcdb231fd33c93f95c22edebe571122c61/chrome/browser/ui/send_tab_to_self/send_tab_to_self_bubble_controller.h
[modify]
https://crrev.com/75362bbcdb231fd33c93f95c22edebe571122c61/chrome/browser/ui/views/send_tab_to_self/send_tab_to_self_bubble_view_impl.h

Comment 31 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:09 PM EDT Project Member

Labels: Release-0-M101

Comment 32 by merc....@gmail.com on Mon, Apr 25, 2022, 9:51 PM EDT

Hi, I want to change my Credit info to: Weipeng Jiang (@Krace) and Guang Gong of 360 Vulnerability Research Institute
Thank you.

Comment 33 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT Project Member

Labels: CVE-2022-1481 CVE_description-missing

Comment 34 by elainechien@chromium.org on Tue, Apr 26, 2022, 8:19 PM EDT Project Member

Cc: elainechien@chromium.org

Comment 35 by ellyj...@chromium.org on Thu, Apr 28, 2022, 2:49 PM EDT Project Member

Cc: victorvianna@google.com

Comment 36 by sheriffbot on Fri, Jul 15, 2022, 1:31 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

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

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

Comment 37 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 38 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing