☆ Starred by 6 users

Owner:	collinbaker@chromium.org **Last visit 17 days ago**
CC:	tluk@chromium.org pbos@chromium.org tbergquist@chromium.org bsep@chromium.org cyan@chromium.org tapted@chromium.org msw@chromium.org connily@chromium.org ellyj...@chromium.org collinbaker@chromium.org erikc...@chromium.org sky@chromium.org est...@chromium.org dfried@chromium.org top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>BookmarksBar
Modified:	Jun 15, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-02-09
OS:	Linux, Windows, Chrome
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-89
Target-88
Target-89
Merge-Rejected-88
merge-merged-4240
merge-merged-86

Issue 1161144: Security: UAF in Bookmark OpenAll

Reported by leecraso@gmail.com on Tue, Dec 22, 2020, 6:29 AM EST

Code

VULNERABILITY DETAILS

When the number of user bookmarks reaches 15, open all[1] bookmarks and a confirmation box[2] will pop up. The MessageBox will run a nested message loop[3] to continue running the ui thread. If the web content or other related instances are destroyed, the UAF will be triggered after the nested message loops exit.

[1].
https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc;l=113;drc=b0d21f299ba5fd0c51c26f1f440fb1a006fc4753
[2].
https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc;l=73;drc=b0d21f299ba5fd0c51c26f1f440fb1a006fc4753
[3]. https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/ui/views/message_box_dialog.cc;l=85;drc=8b5f6ef28dd93e62fc1a75bc7a812af1b33777ec

VERSION
Chrome Version: stable
Operating System: Linux, Windows, ChromeOS

REPRODUCTION CASE
1. Ensure that the current user has more than 15 bookmarks.
2. $ python -m SimpleHTTPServer
   $ out/asan/chrome --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html" "about:blank"
3. Show bookmarks bar on "poc.html", click the trigger button, right-click the bookmark bar and click "open all".
4. Click yes after the page "poc.html" is closed.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State: see asan file

CREDIT INFORMATION
Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab

poc.html
297 bytes View Download

BookmarkOpenAll.asan
16.2 KB Download

Comment 1 by sheriffbot on Tue, Dec 22, 2020, 6:29 AM EST

Labels: reward-potential

Comment 2 by ajgo@google.com on Tue, Dec 22, 2020, 6:56 PM EST

BookmarkOpenAll.asan.txt
16.2 KB View Download

Comment 3 by ajgo@google.com on Tue, Dec 22, 2020, 7:12 PM EST
Cc: pkasting@chromium.org tluk@chromium.org ellyj...@chromium.org msw@chromium.org pbos@chromium.org sky@chromium.org tapted@chromium.org bsep@chromium.org connily@chromium.org cyan@chromium.org dfried@chromium.org erikc...@chromium.org sky@chromium.org tbergquist@chromium.org est...@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable
Components: UI>Browser UI>Browser>TabStrip

Thanks for the report.

Assigning as Medium as this requires significant user interaction.

There have been few changes to this code for a long time. Adding some bookmarks and tabstrip folks that might know who best to point this towards.

Comment 4 by sheriffbot on Wed, Dec 23, 2020, 1:03 PM EST
Labels: Target-88 M-88

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

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

Comment 5 by sheriffbot on Wed, Dec 23, 2020, 1:39 PM EST
Labels: -Pri-3 Pri-1

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

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

Comment 6 by kenrb@chromium.org on Fri, Jan 15, 2021, 1:07 PM EST
Status: Assigned (was: Unconfirmed)
Owner: pkasting@chromium.org
Cc: -pkasting@chromium.org
Labels: OS-Chrome OS-Linux OS-Windows

pkasting@: Can you please help triage this? It appears to be a use-after-free in the browser process, though with some very specific user interaction to trigger it.

Comment 7 by sky@chromium.org on Fri, Jan 15, 2021, 1:15 PM EST
Owner: thomasanderson@chromium.org

pkasting->tom as tom is removing the nested message loop, which should fix this (https://chromium-review.googlesource.com/c/chromium/src/+/2622521).

Comment 8 by adetaylor@google.com on Fri, Jan 15, 2021, 1:56 PM EST
Labels: external_security_report

Comment 9 by bugdroid on Fri, Jan 15, 2021, 8:00 PM EST
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f6658bc4fcfe269c53f8806e02492c658bedb09f

commit f6658bc4fcfe269c53f8806e02492c658bedb09f
Author: Tom Anderson <thomasanderson@chromium.org>
Date: Sat Jan 16 00:59:21 2021

Avoid spinning a nested message loop for X11 clipboard

BUG=443355,~~1138143~~,~~1161141~~,~~1161143~~,~~1161144~~,~~1161145~~,~~1161146~~,~~1161147~~,~~1161149~~,~~1161151~~,~~1161152~~

Change-Id: I5c95a9d066683d18f344d694e517274e3ef7ccb4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2622521
Reviewed-by: Scott Violet <sky@chromium.org>
Commit-Queue: Thomas Anderson <thomasanderson@chromium.org>
Cr-Commit-Position: refs/heads/master@{#844318}

[modify] https://crrev.com/f6658bc4fcfe269c53f8806e02492c658bedb09f/ui/base/x/selection_requestor_unittest.cc
[modify] https://crrev.com/f6658bc4fcfe269c53f8806e02492c658bedb09f/ui/base/x/selection_requestor.cc

Comment 10 by thomasanderson@chromium.org on Fri, Jan 15, 2021, 8:11 PM EST
Status: Fixed (was: Assigned)

Comment 11 by sheriffbot on Sat, Jan 16, 2021, 12:42 PM EST
Labels: reward-topanel

Comment 12 by sheriffbot on Sat, Jan 16, 2021, 1:56 PM EST
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 13 by sheriffbot on Sat, Jan 16, 2021, 2:21 PM EST
Labels: Merge-Request-88

Requesting merge to beta M88 because latest trunk commit (844318) appears to be after beta branch point (827102).

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

Comment 14 by sheriffbot on Sat, Jan 16, 2021, 2:24 PM EST
Labels: -Merge-Request-88 Merge-Review-88 Hotlist-Merge-Review

This bug requires manual review: We are only 2 days from stable.
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: govind@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), srinivassista @(Desktop)

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

Comment 15 by leecraso@gmail.com on Sun, Jan 17, 2021, 9:05 PM EST

It is a very effective patch, but this issue is not related to the clipboard. In this issue, the caller of the nested message is |MessageBoxDialog::Show()=>ShowSync()|, so I think thee patch does not take effect for this issue.

Comment 16 by thomasanderson@chromium.org on Tue, Jan 19, 2021, 2:00 PM EST

Status: Available (was: Fixed)
Owner: ----

Comment 17 by adetaylor@google.com on Wed, Jan 20, 2021, 7:01 PM EST

Labels: -reward-potential

Comment 18 by connily@chromium.org on Fri, Jan 22, 2021, 3:31 PM EST

Cc: collinbaker@chromium.org
Components: -UI>Browser>TabStrip -UI>Browser UI>Browser>TopChrome>BookmarksBar

Comment 19 by collinbaker@chromium.org on Fri, Jan 22, 2021, 5:43 PM EST

Status: Started (was: Available)
Owner: collinbaker@chromium.org

This seems fundamentally broken. chrome::OpenAll() takes a pointer to the active WebContents (through the PageNavigator interface) and the active Browser window (its gfx::NativeWindow). It runs a nested RunLoop then assumes these pointers are valid afterward. Clearly this doesn't always hold true.

The best fix I can think of is to make OpenAll() and friends non-synchronous and instead run a callback This may require some untangling.

Comment 20 by sky@chromium.org on Fri, Jan 22, 2021, 7:12 PM EST

While tedious, you can observe both Browser (via BrowserListObserver) and WebContents (through WebContentsObserver) being destroyed. You could then abort the open if either are destroyed.

Comment 21 by collinbaker@chromium.org on Tue, Jan 26, 2021, 2:32 PM EST

Potential fix at https://chromium-review.googlesource.com/c/chromium/src/+/2650689

Comment 22 by bugdroid on Fri, Feb 5, 2021, 4:12 PM EST

Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/58ae65c7f9a276777e611db69633b2ff8ed32cb7

commit 58ae65c7f9a276777e611db69633b2ff8ed32cb7
Author: Collin Baker <collinbaker@chromium.org>
Date: Fri Feb 05 21:12:29 2021

Make "open all bookmarks" safe

chrome::OpenAll may prompt the user before opening many bookmarks. It
uses a nested RunLoop to do so. However, it takes as arguments
pointers that may be invalid at the end of this RunLoop.

This CL replaces chrome::OpenAll with chrome::OpenAllIfAllowed, which
returns immediately and opens the tabs asynchronously if prompting the
user. Instead of taking a content::PageNavigator pointer directly, it
takes a callback to fetch the pointer after the user acknowledges the
prompt. This can ensure a valid PageNavigator is used.

Another function chrome::OpenAllImmediately is added for tests which
shouldn't open a message box.

~~Fixed: 1161144~~
Change-Id: I6d0d73ec1d9deaf3cb339dc9646d7fe77a27674e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2650689
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Cr-Commit-Position: refs/heads/master@{#851279}

[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/media/webrtc/desktop_capture_access_handler.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_bar_view.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/simple_message_box.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_context_menu_unittest.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/bookmarks/bookmark_context_menu_controller_unittest.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_bar_view.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/process_singleton_win.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/webui/chromeos/cellular_setup/mobile_setup_dialog.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_bar_view_test.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/toolbar/app_menu.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate_unittest.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/message_box_dialog.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_context_menu.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.cc
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/views/bookmarks/bookmark_context_menu.h
[modify] https://crrev.com/58ae65c7f9a276777e611db69633b2ff8ed32cb7/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc

Comment 23 by collinbaker@chromium.org on Fri, Feb 5, 2021, 5:40 PM EST

NextAction: 2021-02-09

I can request a merge to 89 after this is verified

Comment 24 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:32 PM EST

Labels: Merge-Request-89

Sheriffbot made a mistake by requesting merge to M88 but not M89, so I'm filling the gap.

That said, I think this is significantly too complex to meet the bar for an M88 merge (as it's only Medium severity). I'd like to merge to M89 in due course, though.

leecraso@, if you get a chance to confirm that this is fixed, that'd be great.

Comment 25 by sheriffbot on Wed, Feb 10, 2021, 4:33 PM EST
Labels: -Merge-Request-89 Merge-Review-89

This bug requires manual review: M89's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

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

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

Comment 26 Deleted

Comment 27 Deleted

Comment 28 by leecraso@gmail.com on Thu, Feb 11, 2021, 7:31 AM EST

About c24: Since I'm on vacation, sorry for not responding in time. The patch works well in my test.

Comment 29 by adetaylor@chromium.org on Fri, Feb 12, 2021, 12:08 PM EST
Labels: -merge-merged-88 -Merge-Review-89 -merge-merged-4389 -merge-merged-89

Thanks leecraso@ for #c28.

The merges in #c26 and #c27 are actually unrelated to this bug so I'm deleting those comments (there was a mistake in the bug list within the CL).

Comment 30 by adetaylor@chromium.org on Fri, Feb 12, 2021, 12:09 PM EST
Labels: -merge-merged-4324

Comment 31 by adetaylor@chromium.org on Fri, Feb 12, 2021, 12:10 PM EST
Labels: Merge-Approved-89

Approving merge to M89, branch 4389. This should be merged along with ~~issue 1176098~~ which is a problem in the fix.

Comment 32 by adetaylor@google.com on Fri, Feb 12, 2021, 12:35 PM EST
Labels: -Merge-Review-88 Merge-Rejected-88

Rejecting merge to M88. This is too complex a change to merge into M88 at this point in the cycle.

Comment 33 by bugdroid on Fri, Feb 12, 2021, 6:09 PM EST
Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b

commit 4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b
Author: Collin Baker <collinbaker@chromium.org>
Date: Fri Feb 12 23:09:35 2021

Make "open all bookmarks" safe

chrome::OpenAll may prompt the user before opening many bookmarks. It uses a nested RunLoop to do so. However, it takes as arguments pointers that may be invalid at the end of this RunLoop.

This CL replaces chrome::OpenAll with chrome::OpenAllIfAllowed, which returns immediately and opens the tabs asynchronously if prompting the user. Instead of taking a content::PageNavigator pointer directly, it takes a callback to fetch the pointer after the user acknowledges the prompt. This can ensure a valid PageNavigator is used.

Another function chrome::OpenAllImmediately is added for tests which shouldn't open a message box.

(cherry picked from commit 58ae65c7f9a276777e611db69633b2ff8ed32cb7)

~~Fixed: 1161144~~
Change-Id: I6d0d73ec1d9deaf3cb339dc9646d7fe77a27674e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2650689
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#851279}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2693629
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4389@{#994}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/media/webrtc/desktop_capture_access_handler.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.h

[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_bar_view.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/simple_message_box.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_context_menu_unittest.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/bookmarks/bookmark_context_menu_controller_unittest.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_bar_view.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/process_singleton_win.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/webui/chromeos/cellular_setup/mobile_setup_dialog.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_bar_view_test.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/toolbar/app_menu.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate_unittest.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/message_box_dialog.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_context_menu.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.cc
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/views/bookmarks/bookmark_context_menu.h
[modify] https://crrev.com/4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc

Comment 34 by amyressler@google.com on Wed, Feb 17, 2021, 7:12 PM EST

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 35 by amyressler@google.com on Wed, Feb 17, 2021, 7:48 PM EST

Hello, Leecraso and Guang Gong! The VRP Panel has decided to award you $10,000 for this report. Thank you for this submission and your engagement with this issue!

Comment 36 by awhalley@google.com on Fri, Feb 19, 2021, 5:35 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 37 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST

Labels: Release-0-M89

Comment 38 by adetaylor@google.com on Mon, Mar 1, 2021, 7:27 PM EST

Labels: CVE-2021-21167 CVE_description-missing

Comment 39 by vsavu@google.com on Wed, Mar 3, 2021, 6:01 AM EST

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

Comment 40 by gianluca@google.com on Wed, Mar 3, 2021, 10:35 AM EST

Labels: LTS-Merge-Approved-86

Comment 41 by sheriffbot on Wed, Mar 3, 2021, 12:21 PM EST

Labels: -M-88 Target-89 M-89

Comment 42 by Git Watcher on Tue, Mar 9, 2021, 9:23 AM EST

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/77e9baae36b6bf682eaea96931641d7d31ed0f86

commit 77e9baae36b6bf682eaea96931641d7d31ed0f86
Author: Collin Baker <collinbaker@chromium.org>
Date: Tue Mar 09 14:22:02 2021

Make "open all bookmarks" safe

chrome::OpenAll may prompt the user before opening many bookmarks. It
uses a nested RunLoop to do so. However, it takes as arguments
pointers that may be invalid at the end of this RunLoop.

This CL replaces chrome::OpenAll with chrome::OpenAllIfAllowed, which
returns immediately and opens the tabs asynchronously if prompting the
user. Instead of taking a content::PageNavigator pointer directly, it
takes a callback to fetch the pointer after the user acknowledges the
prompt. This can ensure a valid PageNavigator is used.

Another function chrome::OpenAllImmediately is added for tests which
shouldn't open a message box.

[M86 Merge]: Fixed conflics in bookmark_bar_view.*

(cherry picked from commit 58ae65c7f9a276777e611db69633b2ff8ed32cb7)

(cherry picked from commit 4ff0cb3cded4c5a0203e8cf2712a37ef9090f57b)

~~Fixed: 1161144~~
Change-Id: I6d0d73ec1d9deaf3cb339dc9646d7fe77a27674e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2650689
Commit-Queue: Collin Baker <collinbaker@chromium.org>
Reviewed-by: Scott Violet <sky@chromium.org>
Auto-Submit: Collin Baker <collinbaker@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#851279}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2693629
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Original-Commit-Position: refs/branch-heads/4389@{#994}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2731650
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1567}

Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/media/webrtc/desktop_capture_access_handler.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/process_singleton_win.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/bookmarks/bookmark_context_menu_controller.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/bookmarks/bookmark_context_menu_controller_unittest.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/bookmarks/bookmark_utils_desktop.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/bookmarks/bookmark_utils_desktop.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/simple_message_box.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_bar_view.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_bar_view.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_bar_view_test.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_context_menu.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_context_menu.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_context_menu_unittest.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_menu_controller_views.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate.h
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/bookmarks/bookmark_menu_delegate_unittest.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/message_box_dialog.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/views/toolbar/app_menu.cc
[modify] https://crrev.com/77e9baae36b6bf682eaea96931641d7d31ed0f86/chrome/browser/ui/webui/chromeos/cellular_setup/mobile_setup_dialog.cc

Comment 43 by vsavu@google.com on Tue, Mar 9, 2021, 11:03 AM EST

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

Comment 44 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 45 by sheriffbot on Tue, Jun 15, 2021, 1:52 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