Starred by 2 users

Owner:	solomonkinard@chromium.org
CC:	karandeepb@chromium.org solomonkinard@chromium.org tbergquist@chromium.org connily@chromium.org top-chrome-bugs@google.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>TopChrome>TabStrip UI>Browser>TopChrome>TabStrip>TabGroups
Modified:	Sep 15, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-10000
Merge-na
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
Target-89
Target-90
M-91
LTS-Security-86
LTS-Security-NotApplicable-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
Release-0-M91
CVE-2021-30524

Issue 1197146: Security: UAF when extension removes tab group during drag

Reported by derce...@gmail.com on Thu, Apr 8, 2021, 11:54 AM EDT

Code

VULNERABILITY DETAILS
When a tab group is being dragged, if an extension removes that group (e.g. by moving all tabs in the group to another group), a use-after-free will occur in the browser process.

VERSION
Chrome Version: Tested on 91.0.4472.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE
1. Install the attached extension.
2. Move at least one tab into a group and start dragging the group (by dragging the group header).
3. Once the extension detects that a tab has moved (using chrome.tabs.onMoved) and is part of a group, it will move all the tabs in the group to a new group using chrome.tabs.group. This will then cause a use-after-free in the browser process. You can verify that by going through these steps in an asan build.

CREDIT INFORMATION
Reporter credit: David Erceg

asan_output_870481.txt
18.2 KB View Download

background.js
1.1 KB View Download

manifest.json
156 bytes View Download

Comment 1 by sheriffbot on Thu, Apr 8, 2021, 11:56 AM EDT

Labels: external_security_report

Comment 2 by cthomp@chromium.org on Thu, Apr 8, 2021, 2:20 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: dfried@chromium.org
Cc: connily@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>TopChrome>TabStrip>TabGroups UI>Browser>TopChrome>TabStrip

Thanks for the report and the ASAN logs. I've confirmed on Chrome 90 ASAN and Chrome 89 ASAN.

dfried@ this bug is similar to ~~Issue 1196309~~ that I sent your way before, although it appears to have a different root cause. Could you take a look at this one as well or help redirect it to a good owner? Thanks.

I think we should also do some variant analysis for underlying architectural issues here with unexpected interactions with the chrome.tabs API.

Comment 3 by connily@chromium.org on Thu, Apr 8, 2021, 2:23 PM EDT

Owner: tbergquist@chromium.org

This actually looks similar to ~~crbug.com/1195573~~, and likely has the same repro. Assigning to Taylor as well

Comment 4 by sheriffbot on Fri, Apr 9, 2021, 12:47 PM EDT

Labels: Target-89 M-89

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

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

Comment 5 by connily@chromium.org on Tue, Apr 13, 2021, 2:01 PM EDT

Owner: collinbaker@chromium.org
Cc: tbergquist@chromium.org

Comment 6 by sheriffbot on Thu, Apr 15, 2021, 12:21 PM EDT

Labels: -M-89 M-90 Target-90

Comment 7 by collinbaker@chromium.org on Wed, Apr 21, 2021, 5:01 PM EDT

Cc: solomonkinard@chromium.org

Comment 8 Deleted

Comment 9 by solomonkinard@chromium.org on Thu, Apr 29, 2021, 11:59 PM EDT

Status: Started (was: Fixed)

Comment 10 by solomonkinard@chromium.org on Fri, Apr 30, 2021, 12:57 AM EDT

crrev.com/c/2859671

Comment 11 by solomonkinard@chromium.org on Fri, Apr 30, 2021, 4:42 PM EDT

Cc: karandeepb@chromium.org

cc cl reviewer

Comment 12 by Git Watcher on Mon, May 17, 2021, 3:29 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/33109f1824b9ae3d488b7372f9aca68f611be606

commit 33109f1824b9ae3d488b7372f9aca68f611be606
Author: Solomon Kinard <solomonkinard@chromium.org>
Date: Mon May 17 19:28:43 2021

[Extensions][Tabs] Ensure tab strip is editable before editing

~~Bug: 1198747~~,~~1197146~~,1197888,~~1196309~~,~~1202598~~
Change-Id: Ic51669a7f7b17a35cd2c0ed018abcfeddf068a26
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2891080
Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Karan Bhatia <karandeepb@chromium.org>
Cr-Commit-Position: refs/heads/master@{#883567}

[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/test/base/test_browser_window.cc
[modify] https://crrev.com/33109f1824b9ae3d488b7372f9aca68f611be606/chrome/test/base/test_browser_window.h

Comment 13 by solomonkinard@chromium.org on Mon, May 17, 2021, 3:53 PM EDT

Status: Fixed (was: Started)

crrev.com/c/2891080 merged.

Comment 14 by sheriffbot on Tue, May 18, 2021, 12:43 PM EDT

Labels: reward-topanel

Comment 15 by sheriffbot on Tue, May 18, 2021, 2:02 PM EDT

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

Comment 16 by sheriffbot on Tue, May 18, 2021, 2:23 PM EDT

Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (883567) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (883567) appears to be after beta branch point (965).

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

Comment 17 by sheriffbot on Tue, May 18, 2021, 2:26 PM EDT

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: We are only 6 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: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 18 by adetaylor@google.com on Tue, May 18, 2021, 4:13 PM EDT

Labels: -Merge-Request-90 -Merge-Review-91 Merge-NA

Handling merges on ~~issue 1198717~~.

Comment 19 by Git Watcher on Tue, May 18, 2021, 8:10 PM EDT

Labels: merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f5ae8693fcb042797de12b6b9cc055da0090a80a

commit f5ae8693fcb042797de12b6b9cc055da0090a80a
Author: Solomon Kinard <solomonkinard@chromium.org>
Date: Wed May 19 00:09:39 2021

[M91][Extensions][Tabs] Ensure tab strip is editable before editing

(cherry picked from commit 33109f1824b9ae3d488b7372f9aca68f611be606)

~~Bug: 1198717~~,~~1197146~~,1197888,~~1196399~~,~~1202598~~
Change-Id: Ic51669a7f7b17a35cd2c0ed018abcfeddf068a26
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2891080
Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Karan Bhatia <karandeepb@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#883567}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2904568
Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1169}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/test/base/test_browser_window.cc
[modify] https://crrev.com/f5ae8693fcb042797de12b6b9cc055da0090a80a/chrome/test/base/test_browser_window.h

Comment 20 by Git Watcher on Wed, May 19, 2021, 3:42 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7260804a2f0823fdec95e69de0e449bb9fed1f35

commit 7260804a2f0823fdec95e69de0e449bb9fed1f35
Author: Solomon Kinard <solomonkinard@chromium.org>
Date: Wed May 19 19:41:28 2021

[Extensions][Tabs] Include error message if not model isn't editable

See crrev.com/c/2904568.

~~Bug: 1198717~~,~~1197146~~,1197888,~~1196399~~,~~1202598~~
Change-Id: Idc6f1a1e336e08926de75226debcff799d703d00
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2903572
Reviewed-by: Karan Bhatia <karandeepb@chromium.org>
Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>
Cr-Commit-Position: refs/heads/master@{#884626}

[modify] https://crrev.com/7260804a2f0823fdec95e69de0e449bb9fed1f35/chrome/browser/extensions/api/tabs/tabs_api.cc

Comment 21 by amyressler@chromium.org on Mon, May 24, 2021, 11:10 AM EDT

Labels: Release-0-M91

Comment 22 by amyressler@google.com on Mon, May 24, 2021, 2:17 PM EDT

Labels: CVE-2021-30524 CVE_description-missing

Comment 23 by janag...@google.com on Wed, May 26, 2021, 10:56 AM EDT

Cc: janag...@google.com
Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 24 by janag...@google.com on Wed, May 26, 2021, 11:16 AM EDT

Labels: LTS-Security-NotApplicable-86

Not applicable to LTS since tab groups API was added after LTS branch.

Comment 25 by janag...@google.com on Wed, May 26, 2021, 11:17 AM EDT

Labels: -LTS-Merge-Request-86

Comment 26 by janag...@google.com on Wed, May 26, 2021, 11:38 AM EDT

Cc: -janag...@google.com

Comment 27 by amyressler@google.com on Wed, Jun 2, 2021, 3:51 PM EDT

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 28 by amyressler@chromium.org on Wed, Jun 2, 2021, 5:29 PM EDT

Congratulations, David! The VRP Panel has decided to award you $10,000 for this report. (And a couple of others this week, too!)

Comment 29 by amyressler@google.com on Fri, Jun 4, 2021, 10:50 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 30 by asumaneev@google.com on Mon, Jun 7, 2021, 3:16 PM EDT

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 31 by amyressler@google.com on Mon, Jun 7, 2021, 3:26 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Tue, Jun 8, 2021, 12:21 PM EDT

Labels: -M-90 M-91 Target-91

Comment 33 by gianluca@google.com on Wed, Jun 9, 2021, 10:44 AM EDT

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 34 by Git Watcher on Wed, Jun 9, 2021, 11:56 AM EDT

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7aeab825dc9b93ba302d1c124c572213c4967b53

commit 7aeab825dc9b93ba302d1c124c572213c4967b53
Author: Solomon Kinard <solomonkinard@chromium.org>
Date: Wed Jun 09 15:54:57 2021

[M90-LTS][Extensions][Tabs] Ensure tab strip is editable before editing

(cherry picked from commit 33109f1824b9ae3d488b7372f9aca68f611be606)

(cherry picked from commit f5ae8693fcb042797de12b6b9cc055da0090a80a)

~~Bug: 1198717~~,~~1197146~~,1197888,~~1196309~~,~~1203598~~
Change-Id: Ic51669a7f7b17a35cd2c0ed018abcfeddf068a26
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2891080
Commit-Queue: Solomon Kinard <solomonkinard@chromium.org>
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Karan Bhatia <karandeepb@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#883567}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2904568
Auto-Submit: Solomon Kinard <solomonkinard@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4472@{#1169}
Cr-Original-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2944872
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1503}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tab_groups/tab_groups_api.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tab_groups/tab_groups_api_unittest.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_api_unittest.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/api/tabs/tabs_constants.h
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/test/base/test_browser_window.cc
[modify] https://crrev.com/7aeab825dc9b93ba302d1c124c572213c4967b53/chrome/test/base/test_browser_window.h

Comment 35 by asumaneev@google.com on Wed, Jun 9, 2021, 11:58 AM EDT

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 36 by sheriffbot on Wed, Sep 15, 2021, 1:31 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