☆ Starred by 4 users

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

Hotlist-Merge-Review
reward-10000
Security_Impact-Stable
Deadline-Exceeded
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
Target-90
FoundIn-90
M-92
Target-91
Target-92
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515

Issue 1209469: Security: OOB write after creating pinned tab that's also in a group

Reported by derce...@gmail.com on Sat, May 15, 2021, 8:14 AM EDT

Code

VULNERABILITY DETAILS
A pinned tab typically can't be placed in a group. However, if a tab is created within the bounds of an existing group, the tab will be assigned to that group. This is true even if the tab is pinned.

An extension can then use this behavior to produce the same effect as described in ~~issue 1108717~~. Specifically, moving the group will also move the pinned tab, breaking the constraint that pinned tabs are always at the start of the tab strip. Then, attempting to move the pinned tab to a different index will result in an out-of-bounds write in the browser process.

VERSION
Chrome Version: Tested on 92.0.4509.0 (latest asan build)
Operating System: Windows 10, version 20H2

REPRODUCTION CASE
1. Install the attached extension.
2. Once installed, the extension will create a window with three tabs: two that are in a group and one that's not.
3. The extension will then create a new pinned tab using the following call:

chrome.tabs.create({windowId: newWindow.id, index: 1, pinned: true, url: "about:blank"});

Because the specified index is in the middle of the existing group, the tab will be added to that group, even though the tab is pinned.

4. The extension will then call chrome.tabGroups.move to move the group to the end of the tab strip. This will also move the pinned tab, meaning that there's now a pinned tab that's not at the start of the tab strip.
5. Finally, the extension will use chrome.tabs.move to move the pinned tab to index 0. This will result in an OOB write in the browser process.

CREDIT INFORMATION
Reporter credit: David Erceg

asan_output_883253.txt
12.0 KB View Download

manifest.json
196 bytes View Download

service_worker.js
1.0 KB View Download

Comment 1 by derce...@gmail.com on Sat, May 15, 2021, 8:15 AM EDT

The core issue here is that the code that checks whether a new tab should be added to an existing group doesn't check whether the tab is pinned:

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/tabs/tab_strip_model.cc;l=1003;drc=511d2e61f78efa707c00efe3fbdd712b98fc0ebe

Comment 2 by sheriffbot on Sat, May 15, 2021, 8:16 AM EDT Project Member

Labels: external_security_report

Comment 3 by xinghuilu@chromium.org on Mon, May 17, 2021, 1:28 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: solomonkinard@chromium.org
Cc: collinbaker@chromium.org tbergquist@chromium.org cthomp@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>TabStrip

Thanks for the report! Triaging the same way as ~~https://crbug.com/1198717~~.

Comment 4 by xinghuilu@chromium.org on Mon, May 17, 2021, 2:12 AM EDT Project Member

Cc: karandeepb@chromium.org

Comment 5 by sheriffbot on Mon, May 17, 2021, 12:47 PM EDT Project Member

Labels: M-90 Target-90

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 6 by sheriffbot on Wed, May 26, 2021, 12:21 PM EDT Project Member

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

Comment 7 by sheriffbot on Sat, May 29, 2021, 12:21 PM EDT Project Member

solomonkinard: 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 8 by sheriffbot on Sat, Jun 12, 2021, 12:21 PM EDT Project Member

solomonkinard: Uh oh! This issue still open and hasn't been updated in the last 28 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 9 by solomonkinard@chromium.org on Tue, Jun 29, 2021, 2:02 PM EDT Project Member

In me queue, but will ask for someone else to look.

Comment 10 by solomonkinard@chromium.org on Tue, Jun 29, 2021, 4:49 PM EDT Project Member

Owner: ----
Cc: solomonkinard@chromium.org connily@chromium.org dpenning@chromium.org

Comment 11 by solomonkinard@chromium.org on Tue, Jun 29, 2021, 6:39 PM EDT Project Member

Connily mentioned that the tabs team may be able to start to consider this and related p1 bugs tomorrow, as some of the changes may be beyond the scope of the extensions API.

Comment 12 by solomonkinard@chromium.org on Tue, Jun 29, 2021, 6:41 PM EDT Project Member

Owner: connily@chromium.org

Thanks again Connily. Adding as owner so we don't lose track of them.

Comment 13 by rsesek@chromium.org on Wed, Jul 7, 2021, 5:32 PM EDT Project Member

Labels: FoundIn-90
Components: UI>Browser>TopChrome>TabStrip>TabGroups

Comment 14 by dpenning@chromium.org on Thu, Jul 8, 2021, 9:32 PM EDT Project Member

Owner: dpenning@chromium.org

Taking a look at this tommorrow

Comment 15 by Git Watcher on Tue, Jul 13, 2021, 12:06 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e06d6c59ec36066fa8ff9b9874b63c7e189fc1da

commit e06d6c59ec36066fa8ff9b9874b63c7e189fc1da
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Tue Jul 13 04:05:10 2021

Fix case where an extension could open a pinned grouped tab.

~~Bug: 1209469~~
Change-Id: Ib3dea05cbc1f8b29450a336a3089e0e2a6a8e9cf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018421
Commit-Queue: Peter Boström <pbos@chromium.org>
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Commit-Position: refs/heads/master@{#900825}

[modify] https://crrev.com/e06d6c59ec36066fa8ff9b9874b63c7e189fc1da/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 16 by adetaylor@google.com on Tue, Jul 13, 2021, 10:00 PM EDT Project Member

Thanks Taylor! Could you mark this as Fixed if you believe this is a complete fix? So that sheriffbot can do all the merge stuff - https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/security-labels.md#TOC-Merge-labels

Comment 17 by sheriffbot on Wed, Jul 14, 2021, 9:11 AM EDT Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 18 by tbergquist@chromium.org on Wed, Jul 14, 2021, 2:58 PM EDT Project Member

Status: Fixed (was: Assigned)

Yep 100% this should be fully fixed.

Comment 19 by sheriffbot on Thu, Jul 15, 2021, 9:06 AM EDT Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Thu, Jul 15, 2021, 9:11 AM EDT Project Member

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

Comment 21 by sheriffbot on Thu, Jul 15, 2021, 9:11 AM EDT Project Member

Labels: Merge-Request-92 Merge-Request-91

Requesting merge to stable M91 because latest trunk commit (900825) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (900825) appears to be after beta branch point (885287).

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

Comment 22 by sheriffbot on Thu, Jul 15, 2021, 9:13 AM EDT Project Member

Labels: -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: We are only 4 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/+/main/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), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 23 by adetaylor@google.com on Thu, Jul 15, 2021, 2:40 PM EDT Project Member

Let's give this a little more bake time before merging to M92 and aim to merge it for the first security refresh.

Comment 24 by amyressler@google.com on Thu, Jul 22, 2021, 1:05 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 25 by amyressler@google.com on Thu, Jul 22, 2021, 1:09 PM EDT Project Member

Congrats, David-- The VRP Panel has decided to award you $10,000 for this report. Nice work!

Comment 26 by amyressler@google.com on Fri, Jul 23, 2021, 2:16 PM EDT Project Member

Labels: -Merge-Request-91 -Merge-Review-92 Merge-Approved-92 Merge-Approved-91

Approved for merge to M92, please merge to branch 4515 at your earliest convenience.
Also, approved for merge to M91 as this has become the Extended Stable release branch; please also merge to branch 4472. Thank you!

Comment 27 by amyressler@google.com on Fri, Jul 23, 2021, 6:20 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 28 by srinivassista@google.com on Thu, Jul 29, 2021, 3:30 PM EDT Project Member

Status: Assigned (was: Fixed)

re-opening to get engineer attention for the merge

Please merge to M92 asap (before EOD thursday July 29)

Comment 29 by dpenning@chromium.org on Thu, Jul 29, 2021, 4:16 PM EDT Project Member

Cherrypicked https://chromium-review.googlesource.com/c/chromium/src/+/3018421 to M92

Comment 30 by Git Watcher on Thu, Jul 29, 2021, 6:02 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6411996ec3d8211269c1e3e4beabcecdc18dba68

commit 6411996ec3d8211269c1e3e4beabcecdc18dba68
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Thu Jul 29 22:01:52 2021

Fix case where an extension could open a pinned grouped tab.

(cherry picked from commit e06d6c59ec36066fa8ff9b9874b63c7e189fc1da)

~~Bug: 1209469~~
Change-Id: Ib3dea05cbc1f8b29450a336a3089e0e2a6a8e9cf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018421
Commit-Queue: Peter Boström <pbos@chromium.org>
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#900825}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3061459
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: David Pennington <dpenning@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#1917}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/6411996ec3d8211269c1e3e4beabcecdc18dba68/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 31 by amyressler@chromium.org on Fri, Jul 30, 2021, 10:00 AM EDT Project Member

Hello dpenning@, apologies for the ping on another on this morning - but since this issue was discovered in M91, could you please merge to M91 branch 4472, asap for this issue to be a part of the extended stable release since we are moving toward a 4W stable release cycle. Thank you!

Comment 32 by pbos@chromium.org on Fri, Jul 30, 2021, 12:28 PM EDT Project Member

I'll take care of the merge, David's out today.

Comment 33 by Git Watcher on Fri, Jul 30, 2021, 2:34 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/35c7ba7daee91b9cbcdc5e805edb1f96336d2a59

commit 35c7ba7daee91b9cbcdc5e805edb1f96336d2a59
Author: Peter Boström <pbos@chromium.org>
Date: Fri Jul 30 18:33:48 2021

Fix case where an extension could open a pinned grouped tab.

(cherry picked from commit e06d6c59ec36066fa8ff9b9874b63c7e189fc1da)

(cherry picked from commit 6411996ec3d8211269c1e3e4beabcecdc18dba68)

~~Bug: 1209469~~
Change-Id: Ib3dea05cbc1f8b29450a336a3089e0e2a6a8e9cf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018421
Commit-Queue: Peter Boström <pbos@chromium.org>
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Reviewed-by: Peter Boström <pbos@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#900825}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3061459
Reviewed-by: Taylor Bergquist <tbergquist@chromium.org>
Commit-Queue: David Pennington <dpenning@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4515@{#1917}
Cr-Original-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3062587
Reviewed-by: Connie Wan <connily@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1587}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/35c7ba7daee91b9cbcdc5e805edb1f96336d2a59/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 34 by amyressler@chromium.org on Mon, Aug 2, 2021, 10:39 AM EDT Project Member

Labels: Release-1-M92

Comment 35 by amyressler@google.com on Mon, Aug 2, 2021, 10:57 AM EDT Project Member

Labels: CVE-2021-30592 CVE_description-missing

Comment 36 by sheriffbot on Thu, Aug 5, 2021, 1:42 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 37 by sheriffbot on Fri, Aug 6, 2021, 12:22 PM EDT Project Member

Labels: -release-1-m92 -Security_Impact-Extended

This bug is a regression and does not impact stable. Removing incorrectly added Release- labels.

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

Comment 38 by sheriffbot on Fri, Aug 6, 2021, 12:28 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 39 by amyressler@google.com on Fri, Aug 6, 2021, 12:56 PM EDT Project Member

Status: Fixed (was: Assigned)

closing as Fixed as was only re-opened in Comment #28 to get attention for merge to 92 which was achieved. Need Sheriffbot to stop removing valid labels.

Comment 40 by amyressler@google.com on Fri, Aug 6, 2021, 12:57 PM EDT Project Member

Labels: -Security_Impact-Extended Release-1-M92

Comment 41 by sheriffbot on Fri, Aug 6, 2021, 12:59 PM EDT Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 42 by sheriffbot on Fri, Aug 6, 2021, 12:59 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 43 by amyressler@google.com on Fri, Aug 6, 2021, 1:02 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 44 by sheriffbot on Sat, Aug 7, 2021, 12:21 PM EDT Project Member

Labels: -release-1-m92 -Security_Impact-Extended

This bug is a regression and does not impact stable. Removing incorrectly added Release- labels.

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

Comment 45 by sheriffbot on Sat, Aug 7, 2021, 12:25 PM EDT Project Member

Status: Assigned (was: Fixed)

Dear owner, thanks for fixing this bug. We've reopened it because security bugs need Security_Severity and FoundIn labels set, which will enable the bots to request merges to the correct branches (as well as helping out our vulnerability reward and CVE processes). Please consult with any Chrome security contact (security@chromium.org) to arrange to set these labels and then this bug can be marked closed again. Thank you! Severity guidelines: https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md#severity-guidelines-for-security-issues FoundIn guidelines: https://chromium.googlesource.com/chromium/src/+/main/docs/security/security-labels.md#labels-relevant-for-any-type_bug_security Thanks for your time!

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

Comment 46 by sheriffbot on Sat, Aug 7, 2021, 12:25 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 47 by adetaylor@google.com on Sat, Aug 7, 2021, 4:52 PM EDT Project Member

Status: Fixed (was: Assigned)
Labels: Release-1-M92

Apologies for label change spam - this was a bug in our changes to make Sheriffbot work with the Extended Stable branch.

Comment 48 by rzanoni@google.com on Wed, Aug 11, 2021, 6:10 AM EDT Project Member

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

Comment 49 by sheriffbot on Wed, Aug 11, 2021, 12:21 PM EDT Project Member

Labels: -M-91 Target-92 M-92

Comment 50 by rzanoni@google.com on Thu, Aug 19, 2021, 11:30 AM EDT Project Member

Labels: LTS-Size-Small LTS-Complexity-Minimal

Comment 51 by gianluca@google.com on Fri, Aug 20, 2021, 3:34 AM EDT Project Member

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

Comment 52 by Git Watcher on Fri, Aug 20, 2021, 1:38 PM EDT Project Member

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

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/4a94360783033db3b52d8a03f408e6839a25b660

commit 4a94360783033db3b52d8a03f408e6839a25b660
Author: Taylor Bergquist <tbergquist@chromium.org>
Date: Fri Aug 20 17:37:48 2021

[M90-LTS] Fix case where an extension could open a pinned grouped tab.

(cherry picked from commit e06d6c59ec36066fa8ff9b9874b63c7e189fc1da)

~~Bug: 1209469~~
Change-Id: Ib3dea05cbc1f8b29450a336a3089e0e2a6a8e9cf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3018421
Commit-Queue: Peter Boström <pbos@chromium.org>
Auto-Submit: Taylor Bergquist <tbergquist@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#900825}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3086688
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1571}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/4a94360783033db3b52d8a03f408e6839a25b660/chrome/browser/ui/tabs/tab_strip_model.cc

Comment 53 by rzanoni@google.com on Mon, Aug 23, 2021, 4:06 AM EDT Project Member

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

Comment 54 by amyressler@google.com on Thu, Aug 26, 2021, 1:09 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 55 by sheriffbot on Mon, Nov 15, 2021, 1:35 PM EST 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