Starred by 4 users

Owner:	rouslan@chromium.org
CC:	adetaylor@chromium.org danyao@chromium.org pbomm...@chromium.org jinho...@samsung.com srinivassista@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Payments
Modified:	Jul 18, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
reward-20000
CVE_description-submitted
M-81
Target-81
VulnerabilityAnalysis-Requested
VulnerabilityAnalysis-Submitted
M-83
Target-83
merge-merged-4044
merge-merged-81
merge-merged-4103
merge-merged-83
Release-2-M81
CVE-2020-6459

Issue 1065298: UAF in base::SupportsUserData::SetUserData

Reported by cdsrc...@gmail.com on Fri, Mar 27, 2020, 1:34 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

Steps to reproduce the problem:
1 python3.6m -m http.server 8605
2 ./chrome --user-dir=/tmp/nonexist --incognito http://127.0.0.1:8605/crash.html
3 Close the browser manually.

What is the expected behavior?

What went wrong?
Received signal 11 SEGV_MAPERR ffffbbfae73e631
#0 0x55f2c0ac9229 base::debug::CollectStackTrace()
#1 0x55f2c0a2f5b3 base::debug::StackTrace::StackTrace()
#2 0x55f2c0ac8d71 base::debug::(anonymous namespace)::StackDumpSignalHandler()
#3 0x7f89845bb890 <unknown>
#4 0x55f2c0a73b8b base::SupportsUserData::SetUserData()
#5 0x55f2bee3990e content::BrowserContext::GetPermissionController()
#6 0x55f2bf0d248f content::(anonymous namespace)::CheckPermissionForPaymentApps()
#7 0x55f2bf0d6fe4 base::internal::Invoker<>::RunOnce()
#8 0x55f2bf0d5d38 base::internal::Invoker<>::RunOnce()
#9 0x55f2c0a7642b base::TaskAnnotator::RunTask()
#10 0x55f2c0a86e9e base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl()
#11 0x55f2c0a86c51 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoSomeWork()
#12 0x55f2c0a45667 base::(anonymous namespace)::WorkSourceDispatch()
#13 0x7f89826d8417 g_main_context_dispatch
#14 0x7f89826d8650 <unknown>
#15 0x7f89826d86dc g_main_context_iteration
#16 0x55f2c0a454c2 base::MessagePumpGlib::Run()
#17 0x55f2c0a87719 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run()
#18 0x55f2c0a5eda2 base::RunLoop::Run()
#19 0x55f2c06afd83 ChromeBrowserMainParts::MainMessageLoopRun()
#20 0x55f2bee4af8b content::BrowserMainLoop::RunMainMessageLoopParts()
#21 0x55f2bee4cf32 content::BrowserMainRunnerImpl::Run()
#22 0x55f2bee47e9d content::BrowserMain()
#23 0x55f2c0643f35 content::ContentMainRunnerImpl::RunServiceManager()
#24 0x55f2c0643c3a content::ContentMainRunnerImpl::Run()
#25 0x55f2c0692f93 service_manager::Main()
#26 0x55f2c0642011 content::ContentMain()
#27 0x55f2be24c5ae ChromeMain
#28 0x7f897e54ab97 __libc_start_main
#29 0x55f2be24c3ea _start
r8: 00007ffce53e68b8 r9: 0000000000000001 r10: 00007ffce53e6470 r11: 0000000000000001
r12: 00000442fe287990 r13: 000055f2bcb62210 r14: 00000442f771c9d0 r15: 00000442f771c9c0
di: 0000000000000030 si: ffffffffffde1d1 bp: 00007ffce53e6700 bx: 00000442f771c9d0

dx: 0000000000000030 ax: ffffffbbfae73e631 cx: 00007f8984baa000 sp: 00007ffce53e66c0
ip: 000055f2c0a73b8b efl: 0000000000010202 cgf: 002b000000000033 erf: 0000000000000005
trp: 000000000000000e msk: 0000000000000000 cr2: ffffffbbfae73e631
[end of stack trace]
Calling _exit(1). Core file will not be generated.

Did this work before? N/A

Chrome version: Chromium 83.0.4095.0 Channel: stable
OS Version: Ubuntu18.04
Flash Version:

Comment 1 by cdsrc...@gmail.com on Fri, Mar 27, 2020, 1:34 AM EDT

poc.zip
4.9 KB Download

Comment 2 by jdeblasio@chromium.org on Fri, Mar 27, 2020, 12:30 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: rouslan@chromium.org
Cc: danyao@chromium.org
Labels: Security_Severity-High Security_Impact-Stable M-80 Pri-1
Components: Blink>Payments

Thanks for the report.

rouslan@: Can you take a look at this report? All CCing danyao@ for visibility.

It's not clear to me how controllable this is, but the failed check (see below) is in the browser process, so assigning Sev-High. It may be worse.

It took me a while to be able to reproduce this, and I can only do so in trunk, but conservatively setting Security_Impact-Stable until someone can look a bit more at it.

Loading the PoC causes Chrome to hang for a while. Trying to close Chrome during this time usually triggers the crash. If you wait too long (>10 seconds?), it's more likely to not crash.

Comment 3 by rouslan@chromium.org on Fri, Mar 27, 2020, 1:00 PM EDT

Do we have any crash identifiers from chrome://crashes?

CheckPermissionForPaymentApps() uses a raw pointer for browser_context. Is that pointer null or something else?

Comment 4 by rouslan@chromium.org on Fri, Mar 27, 2020, 4:24 PM EDT

Stack seems to suggest that browser_context is null. It does not seem to have a weak pointer. What's the standard procedure for checking whether the browser context is gone?

Comment 5 by rouslan@chromium.org on Sat, Mar 28, 2020, 4:08 PM EDT

Cc: jinho...@samsung.com

Jinho: Do you have any suggestions on how to fix this "use after free"? It appears that browser_context can be freed before CheckPermissionForPaymentApps() is called.

Comment 6 Deleted

Comment 7 by jinho...@samsung.com on Mon, Mar 30, 2020, 1:13 PM EDT

rouslan@,

Since the main() function is called recursively in the attached JS code, it seems that the process is terminated and the BrowserContext is also destroyed. To track the BrowserContext's life, we might make the PaymentAppProvider to KeyedService or might use ChildProcessSecurityPolicy.
However, I think the root cause is that the PaymentRequest constructor in JS side calls GetAllPaymentApps() internally. Since the constructor is not asynchronous, we should defer to call the GetAllPaymentApps() until canMakePayment() or show() is called.

```
try {
  new PaymentRequest([{ supportedMethods: "https://xxxxx.com/pay" }], ..., {});
} catch (e) {
  // The "https://xxxxx.com/pay" causes some error but JS authors can't catch it.
}
```
One workaround might be that we make the JS context stop in the error situation.

Comment 8 by rouslan@google.com on Tue, Apr 7, 2020, 6:06 AM EDT

I plan to look into it this sprint.

Comment 9 by rouslan@google.com on Thu, Apr 9, 2020, 9:05 AM EDT

https://chromium-review.googlesource.com/2144311 is WIP

Comment 10 by adetaylor@google.com on Thu, Apr 9, 2020, 12:18 PM EDT

Thanks for keeping this crbug updated with your progress - it's much appreciated.

Comment 11 by sheriffbot on Thu, Apr 9, 2020, 12:27 PM EDT

Labels: -M-80 Target-81 M-81

Comment 12 by bugdroid on Sat, Apr 11, 2020, 11:24 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/2d0aad1e7602a7076d86772cc159b891cf2cf03b

commit 2d0aad1e7602a7076d86772cc159b891cf2cf03b
Author: Rouslan Solomakhin <rouslan@chromium.org>
Date: Sat Apr 11 15:19:59 2020

[Web Payment] Browser context owned callback.

Before this patch, an unowned function pointer would be invoked
asynchronously with a reference to the possibly freed reference to the
browser context, which could cause use after free in certain
circumstances.

This patch makes the browser context own the callback and binds the
function with a weak pointer, so freeing the browser context invalidates
the weak pointer, which cancels the callback execution.

After this patch, freeing the browser context aborts the asynchronous
callback that dereferences the browser context, so the use after free
is prevented.

~~Bug: 1065209~~
Change-Id: Id6de3099a55c4505e94a8a6d21fb25d6d2b34c6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2144311
Reviewed-by: Danyao Wang <danyao@chromium.org>
Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Commit-Position: refs/heads/master@{#758404}

[modify] https://crrev.com/2d0aad1e7602a7076d86772cc159b891cf2cf03b/content/browser/payments/payment_app_provider_impl.cc

Comment 13 by rouslan@google.com on Sat, Apr 11, 2020, 2:32 PM EDT

Status: Fixed (was: Assigned)

cdsrc2016@ and/or jdeblasio@: Can you please double-check that the bug no longer reproduces after https://chromiumdash.appspot.com/commit/2d0aad1e7602a7076d86772cc159b891cf2cf03b ?

Comment 14 by sheriffbot on Sun, Apr 12, 2020, 2:00 PM EDT

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

Comment 15 by sheriffbot on Sun, Apr 12, 2020, 2:20 PM EDT

Labels: Merge-Request-81

Requesting merge to stable M81 because latest trunk commit (758404) appears to be after stable branch point (737173).

Requesting merge to beta M81 because latest trunk commit (758404) appears to be after beta branch point (737173).

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

Comment 16 by sheriffbot on Sun, Apr 12, 2020, 2:22 PM EDT

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 17 by cdsrc...@gmail.com on Mon, Apr 13, 2020, 12:40 AM EDT

Hhi，@rouslan
After patch in c#12, no uaf reproduced anymore(tried 10+times).

Comment 18 by rouslan@google.com on Mon, Apr 13, 2020, 5:34 AM EDT

Thank you, cdsrc2016@.

Comment 19 by rouslan@google.com on Mon, Apr 13, 2020, 5:35 AM EDT

> 1. Does your merge fit within the Merge Decision Guidelines?

Yes.

> 2. Links to the CLs you are requesting to merge.

https://crrev.com/c/2144311

> 3. Has the change landed and been verified on master/ToT?

Yes.

> 4. Why are these changes required in this milestone after branch?

Fixing a security bug.

> 5. Is this a new feature?

No.

> 6. If it is a new feature, is it behind a flag using finch?

N/A.

Comment 20 by pbommana@google.com on Mon, Apr 13, 2020, 12:00 PM EDT

Cc: adetaylor@chromium.org srinivassista@chromium.org pbomm...@chromium.org
Labels: M-83 Target-83

Please request M83 merge and adding Adetaylor(Security TPM)

Comment 21 by rouslan@google.com on Mon, Apr 13, 2020, 12:03 PM EDT

Labels: Merge-Request-83

Requesting M-83 merge. Thank you for the reminder.

Comment 22 by sheriffbot on Mon, Apr 13, 2020, 12:07 PM EDT

Labels: -Merge-Request-83 Merge-Review-83

This bug requires manual review: To minimize risk and increase branch stability, all merge requests are being reviewed manually by the release team.
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), cindyb@(ChromeOS), srinivassista@(Desktop)

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

Comment 23 by srinivassista@google.com on Mon, Apr 13, 2020, 1:28 PM EDT

Labels: -Merge-Review-83 Merge-Approved-83

Merge approved for M-83, branch:4103, Please merge your changes asap so we can include in dev RC for tomorrow (before 2pm PST)

adetaylor@ FYI

Comment 24 by natashapabrai@google.com on Mon, Apr 13, 2020, 2:37 PM EDT

Labels: reward-topanel

Comment 25 by rouslan@google.com on Mon, Apr 13, 2020, 2:43 PM EDT

Does anyone have any idea what's happening with drover?

$ git-drover --cherry-pick 2d0aad1e7602a7076d86772cc159b891cf2cf03b --branch 4103
Going to cherry-pick
"""
b'commit 2d0aad1e7602a7076d86772cc159b891cf2cf03b\nAuthor: Rouslan Solomakhin <rouslan@chromium.org>\nDate: Sat Apr 11 15:19:59 2020 +0000\n\n [Web Payment] Browser context owned callback.\n \n Before this patch, an unowned function pointer would be invoked\n asynchronously with a reference to the possibly freed reference to the\n browser context, which could cause use after free in certain\n circumstances.\n \n This patch makes the browser context own the callback and binds the\n function with a weak pointer, so freeing the browser context invalidates\n the weak pointer, which cancels the callback execution.\n \n After this patch, freeing the browser context aborts the asynchronous\n callback that dereferences the browser context, so the use after free\n is prevented.\n \n ~~Bug: 1065298~~\n Change-Id: Id6de3099a55c4505e94a8a6d21fb25d6d2b34c6c\n Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2144311\n Reviewed-by: Danyao Wang <danyao@chromium.org>\n Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>\n Cr-Commit-Position: refs/heads/master@{#758404}\n"""
to 4103. Continue (y/n)? y
Traceback (most recent call last):
  File "/home/rouslan/depot_tools/git_drover.py", line 466, in <module>
    main()
  File "/home/rouslan/depot_tools/git_drover.py", line 457, in main
    cherry_pick_change(options.branch, options.cherry_pick,
  File "/home/rouslan/depot_tools/git_drover.py", line 379, in cherry_pick_change
    drover.run()
  File "/home/rouslan/depot_tools/git_drover.py", line 146, in run
    self._run_internal()
  File "/home/rouslan/depot_tools/git_drover.py", line 155, in _run_internal
    self._create_checkout()
  File "/home/rouslan/depot_tools/git_drover.py", line 236, in _create_checkout
    parent_git_dir = os.path.join(self._parent_repo, self._run_git_command(
  File "/home/rouslan/.vpython-root/037449/lib/python3.8/posixpath.py", line 90, in join
    genericpath._check_arg_types('join', a, *p)
  File "/home/rouslan/.vpython-root/037449/lib/python3.8/genericpath.py", line 155, in _check_arg_types
    raise TypeError("Can't mix strings and bytes in path components") from None
TypeError: Can't mix strings and bytes in path components

Comment 26 by rouslan@google.com on Mon, Apr 13, 2020, 2:55 PM EDT

Drover worked on my workstation: https://crrev.com/c/2147843 is being submitted to branch 4103.

Comment 27 by bugdroid on Mon, Apr 13, 2020, 4:51 PM EDT

Labels: -merge-approved-83 merge-merged-4103 merge-merged-83

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/f6ead152294500077ca301af55ac404e17e14f62

commit f6ead152294500077ca301af55ac404e17e14f62
Author: Rouslan Solomakhin <rouslan@chromium.org>
Date: Mon Apr 13 20:49:46 2020

[Merge M83][Web Payment] Browser context owned callback.

Before this patch, an unowned function pointer would be invoked
asynchronously with a reference to the possibly freed reference to the
browser context, which could cause use after free in certain
circumstances.

This patch makes the browser context own the callback and binds the
function with a weak pointer, so freeing the browser context invalidates
the weak pointer, which cancels the callback execution.

After this patch, freeing the browser context aborts the asynchronous
callback that dereferences the browser context, so the use after free
is prevented.

TBR=rouslan@chromium.org

(cherry picked from commit 2d0aad1e7602a7076d86772cc159b891cf2cf03b)

~~Bug: 1065298~~
Change-Id: Id6de3099a55c4505e94a8a6d21fb25d6d2b34c6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2144311
Reviewed-by: Danyao Wang <danyao@chromium.org>
Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#758404}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2147843
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4103@{#109}
Cr-Branched-From: 8ad47e8d21f6866e4a37f47d83a860d41debf514-refs/heads/master@{#756066}

[modify] https://crrev.com/f6ead152294500077ca301af55ac404e17e14f62/content/browser/payments/payment_app_provider_impl.cc

Comment 28 by adetaylor@google.com on Wed, Apr 15, 2020, 3:45 PM EDT

Labels: -Merge-Review-81 Merge-Approved-81

rouslan@, approving merge also to M81 branch 4044. Please have a look to see there are no new crashes in this area on Canary (it looks like it probably also made it into the dev release 83.0.4103.14).

Comment 29 by rouslan@chromium.org on Wed, Apr 15, 2020, 5:19 PM EDT

The crash database contains 4 crash reports with this eact signature in the following versions:
1 report in 74.0.3729.136
2 reports in 79.0.3945.93
1 report in 79.0.3945.116

When looking for all crash stacks that contain CheckPermissionForPaymentApps, but not necessarily this exact stack trace, then there're 51 total reports with the latest being in 80.0.3987.137.

Both queries show no crashes M81 and later, but that could be because of a small sample size: about 1 crash per week.

I'm going ahead and merging into M81 because the fix should be safe.

Comment 30 by natashapabrai@google.com on Wed, Apr 15, 2020, 6:50 PM EDT

Labels: -reward-topanel reward-unpaid reward-20000

*** 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 31 by natashapabrai@google.com on Wed, Apr 15, 2020, 6:52 PM EDT

Congrats! The Panel decided to award you $20,000 for this report!

Comment 32 by natashapabrai@google.com on Wed, Apr 15, 2020, 6:55 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 33 by bugdroid on Wed, Apr 15, 2020, 7:03 PM EDT

Labels: -merge-approved-81 merge-merged-81 merge-merged-4044

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/686d1bfbcb8f4fc0f1c45f1dea61f41730961b4a

commit 686d1bfbcb8f4fc0f1c45f1dea61f41730961b4a
Author: Rouslan Solomakhin <rouslan@chromium.org>
Date: Wed Apr 15 23:03:07 2020

[Merge M81][Web Payment] Browser context owned callback.

Before this patch, an unowned function pointer would be invoked
asynchronously with a reference to the possibly freed reference to the
browser context, which could cause use after free in certain
circumstances.

This patch makes the browser context own the callback and binds the
function with a weak pointer, so freeing the browser context invalidates
the weak pointer, which cancels the callback execution.

After this patch, freeing the browser context aborts the asynchronous
callback that dereferences the browser context, so the use after free
is prevented.

TBR=rouslan@chromium.org

(cherry picked from commit 2d0aad1e7602a7076d86772cc159b891cf2cf03b)

~~Bug: 1065209~~
Change-Id: Id6de3099a55c4505e94a8a6d21fb25d6d2b34c6c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2144311
Reviewed-by: Danyao Wang <danyao@chromium.org>
Commit-Queue: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#758404}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2151474
Reviewed-by: Rouslan Solomakhin <rouslan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4044@{#942}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/686d1bfbcb8f4fc0f1c45f1dea61f41730961b4a/content/browser/payments/payment_app_provider_impl.cc

Comment 34 by adetaylor@google.com on Mon, Apr 20, 2020, 4:32 PM EDT

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

I'm assuming this affects more platforms than just Linux. Please fix if not.

Comment 35 by adetaylor@google.com on Mon, Apr 20, 2020, 4:34 PM EDT

Labels: Release-2-M81

Comment 36 by adetaylor@chromium.org on Mon, Apr 20, 2020, 5:31 PM EDT

Labels: CVE-2020-6459 CVE_description-missing

Comment 37 by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 38 by mmoroz@chromium.org on Tue, Jun 30, 2020, 6:40 PM EDT

Labels: VulnerabilityAnalysis-Requested

rouslan@, thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: https://forms.gle/VWKDUv9a8GXCCRWm7

Comment 39 by rouslan@google.com on Mon, Jul 13, 2020, 9:04 AM EDT

Done!

Comment 40 by mmoroz@google.com on Tue, Jul 14, 2020, 7:38 PM EDT

Labels: VulnerabilityAnalysis-Submitted

Comment 41 by sheriffbot on Sat, Jul 18, 2020, 3:00 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