

☆ Starred by 6 users


Owner:

curranmax@chromium.org


CC:

robertogden@chromium.org


jianli@chromium.org

 buettner@chromium.org


tbansal@chromium.org


 creis@chromium.org

ryansturm@chromium.org

 bengr@chromium.org

curranmax@chromium.org

 carlosk@chromium.org

 nasko@chromium.org

wfh@chromium.org

ajgo@chromium.org

Status:

Fixed (Closed)

Components:

UI>Browser>Offline
Internals>Sandbox>Sitelisolation

Modified:

Aug 26, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Android

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review

Security_Impact-Stable

Deadline-Exceeded

Security_Severity-High

allpublic

CVE_description-submitted

M-90

Target-90

merge-merged-4240

LTS-Security-86

LTS-Merge-Approved-86

merge-merged-4430

merge-merged-90


merge-merged-4472

merge-merged-91

merge-merged-4430_101

Issue 1178202: Security: X-Chrome-offline allows arbitrary file reads from compromised renderer.

Reported by [ahuff...@microsoft.com](#) on Sat, Feb 13, 2021, 8:29 PM EST Project Member

 Code

VULNERABILITY DETAILS

The X-Chrome-offline header is used by the OfflinePageURLLoaderRequestInterceptor to swap out a request with the offline contents. Normally, the user cannot control the headers of a top level navigation. However, this is possible from a compromised renderer by manually specifying the header in a BeginNavigation Mojo call.

If the user has a page download on the same origin as the compromised render process, then this can be abused to read arbitrary files on the device by using the "file_url_intent" reason and specifying an arbitrary path as the "intent_url."

VERSION

Chrome Version: 88.0.4324.155 + stable
Operating System: Android 10

REPRODUCTION CASE

1) Apply the provided patch and rebuild the browser to simulate a compromised renderer.

2) Visit the provided app.js.

3) Download the page.

4) Click the link on the page.

5) The contents of /data/data/org.chromium.chrome/app_chrome/Default/Cookies will be written to the page.

CREDIT INFORMATION

Reporter credit: Alison Huffman, Microsoft Browser Vulnerability Research

app.js

1.1 KB [View](#) [Download](#)

patch.diff

1.3 KB [View](#) [Download](#)

video.webm

1.4 MB [View](#) [Download](#)

0:00 / 0:22

Comment 1 by rsesek@chromium.org on Mon, Feb 15, 2021, 3:42 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: janli@chromium.org

Cc: carlosk@chromium.org

Labels: Security_Impact-Stable Security_Severity-Medium M-89 Pri-1

Thanks for the report.

Comment 2 by rsesek@chromium.org on Mon, Feb 15, 2021, 5:37 PM EST Project Member

Components: UI>Browser>Offline

Comment 3 by [sheriffbot](#) on Tue, Mar 2, 2021, 12:21 PM EST Project Member

janli: Uh oh! This issue still open and hasn't been updated in the last 16 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 4 by [sheriffbot](#) on Thu, Mar 11, 2021, 11:15 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 5 by janli@chromium.org on Thu, Mar 11, 2021, 4:14 PM EST Project Member

We probably need to check `offline_page_request_handler.cc` on how intent file is handled.

Comment 6 by janli@chromium.org on Thu, Mar 11, 2021, 4:32 PM EST Project Member

I tried the above steps and couldn't repro this. Anyone can repro this?

Comment 7 by ahuff...@microsoft.com on Thu, Mar 11, 2021, 5:23 PM EST Project Member

I will not have a build that I can test with again until tomorrow morning. I can reverify then and report back.

Comment 8 by janli@chromium.org on Thu, Mar 11, 2021, 5:52 PM EST Project Member

Cc: bengr@chromium.org

Comment 9 by bengr@chromium.org on Thu, Mar 11, 2021, 5:58 PM EST Project Member

Cc: tbansal@chromium.org

Comment 10 by ahuff...@microsoft.com on Thu, Mar 11, 2021, 6:46 PM EST Project Member

I just re-built the HEAD of main with the supplied changes and it seems its even easier to trigger now. Before it only would work if a download was created through the offline page mechanism. The download page UI seems to have been removed and this now works with any download on the origin.

With the currently supplied POC you should be able to trigger it by.

- 1) Applying the patch to `render_frame_impl.cc`
- 2) Run `adb reverse tcp:3000 tcp:3000`
- 3) `node app.js` (or however you would like to host the html file)
- 5) Visit `127.0.0.1:3000`
- 6) Long press on "Then Click Me" and press download link.
- 7) Once the download completes click the "Then Click Me" link.
- 8) The contents of the cookie database should be open in the `127.0.0.1:3000` origin.

Keep in mind that this feature also exposes a `content_url_intent` reason as well. I have not tested this, but since this exposes the resolution of `content://` urls, if the browser has already been authorized access to the users contacts through `navigator.contacts.select`, it is possible they could use this bug to dump the users contact database from the compromised renderer.

Note: I do not believe the user interaction above is required in an actual compromised renderer.

Comment 11 by tbansal@chromium.org on Thu, Mar 11, 2021, 7:06 PM EST Project Member

Cc: ryansturm@chromium.org curranmax@chromium.org

Comment 12 by tbansal@chromium.org on Thu, Mar 11, 2021, 7:09 PM EST Project Member

Cc: buettner@chromium.org

Comment 13 by tbansal@chromium.org on Thu, Mar 11, 2021, 7:14 PM EST Project Member

Owner: curranmax@chromium.org

Cc: janli@chromium.org

Max, can I assign this to you? Please feel free to reach out to Ryan for a potential fix.

Comment 14 by curranmax@chromium.org on Thu, Mar 25, 2021, 5:23 PM EDT Project Member

Status: Started (was: Assigned)

Comment 15 by tbansal@chromium.org on Thu, Apr 1, 2021, 2:59 PM EDT Project Member

Cc: robertogden@chromium.org

Comment 16 by rsesek@chromium.org on Wed, Apr 7, 2021, 12:11 PM EDT Project Member

Labels: -Security_Severity-Medium Security_Severity-High

Comment 17 by creis@chromium.org on Thu, Apr 8, 2021, 3:58 AM EDT Project Member

Cc: nasko@chromium.org creis@chromium.org

Components: Internals>Sandbox>SiteIsolation

Sounds like Max is discussion solution ideas with Nasko, etc. Adding Site Isolation component for more visibility. Thanks!

Comment 18 by sheriffbot on Thu, Apr 15, 2021, 12:22 PM EDT Project Member

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

Comment 19 by sheriffbot on Thu, Apr 15, 2021, 2:05 PM 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 20 by Git Watcher on Tue, Apr 27, 2021, 9:38 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+f84c79a85f49295be97af1a3dc021c333710501d>

commit `f84c79a85f49295be97af1a3dc021c333710501d`

Author: Max Curran <curranmax@chromium.org>

Date: Wed Apr 28 01:37:54 2021

Cancels requests from the renderer with the X-Chrome-offline header.

This CL adds a `OfflinePageNavigationThrottle` which catches any renderer initiated requests that include the "X-Chrome-offline" header, and then cancels these requests. There is no legitimate reason for a renderer to make a request with this header, but a compromised renderer could add this header in order to read an arbitrary file.

Doc with more details: https://docs.google.com/document/d/1Hh_NQXo6IsRkgZaHeAEKmcDWRZXIDQYvLUKaRyVv6iQ/edit?usp=sharing

Bug-1478203

Change-Id: I5e1a83d68b521db33118ba74e98b8565b02ae6eb
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2840903>
Commit-Queue: Max Curran <curranmax@chromium.org>
Reviewed-by: Robert Ogden <robertogden@chromium.org>
Cr-Commit-Position: refs/heads/master@{#876861}

[modify] <https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/browser/BUILD.gn>
[modify] https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/browser/chrome_content_browser_client.cc
[add] https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/browser/offline_pages/offline_page_navigation_throttle.cc
[add] https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/browser/offline_pages/offline_page_navigation_throttle.h
[add] https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/browser/offline_pages/offline_page_navigation_throttle_unittest.cc
[modify] <https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/chrome/test/BUILD.gn>
[modify] <https://crrev.com/f84c79a85f49295be97af1a3dc021c333710501d/tools/metrics/histograms/xml/offline/histograms.xml>

Comment 21 by curranmax@chromium.org on Wed, May 5, 2021, 5:23 PM EDT Project Member

Labels: Merge-Request-91

Comment 22 by [sheriffbot](#) on Wed, May 5, 2021, 5:27 PM EDT Project Member

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

This bug requires manual review: M91'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), bindusuvama@(iOS), marinakz@(ChromeOS), pbonmana@(Desktop)

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

Comment 23 by curranmax@chromium.org on Wed, May 5, 2021, 5:35 PM EDT Project Member

1. Yes.
2. <https://chromium-review.googlesource.com/c/chromium/src/+2840903>
3. Yes.
4. No.
5. This CL is a fix for a severity-high security bug.
6. No.
7. N/A

Comment 24 by adetaylor@chromium.org on Wed, May 5, 2021, 6:04 PM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-90 Merge-Approved-91

Please mark bugs as Fixed if they're fixed: <https://chromium.googlesource.com/chromium/src/+master/docs/security/security-labels.md#TOC-Merge-labels> or Sheriffbot
can't make the correct decisions about which branches to merge to.

Had this been marked fixed, sheriffbot would have requested merge to M90 and M91.

So, approving merge to M90, branch 4430, and M91, branch 4472, as it looks like this has had reasonable time in Canary even though it's a fairly complex addition.

For M90, please merged by EOD PDT tomorrow (Thursday) so it can be included in next week's security refresh. Thanks!

Finally, please could you fix the OS field - I assume this bug isn't Android-specific? The release TPMs rely on that field in order to determine which branches to merge fixes into.

Comment 25 by curranmax@chromium.org on Wed, May 5, 2021, 6:39 PM EDT Project Member

Status: Fixed (was: Started)

This is Android only, since offline-pages is Android only.

Comment 26 by adetaylor@google.com on Thu, May 6, 2021, 12:57 PM EDT Project Member

OK cool. Thanks.

Comment 27 by [Git Watcher](#) on Thu, May 6, 2021, 1:17 PM EDT Project Member

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

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+3561caa4e0546a2968ade20e2c86ef48080845da>

commit [3561caa4e0546a2968ade20e2c86ef48080845da](https://chromium.googlesource.com/chromium/src/+3561caa4e0546a2968ade20e2c86ef48080845da)
Author: Max Curran <curranmax@chromium.org>
Date: Thu May 06 17:16:25 2021

Cancels requests from the renderer with the X-Chrome-offline header.

This CL adds a OfflinePageNavigationThrottle which catches any renderer initiated requests that include the "X-Chrome-offline" header, and then cancels these requests. There is no legitimate reason for a renderer to make a request with this header, but a compromised renderer could add this header in order to read an arbitrary file.

Doc with more details: https://docs.google.com/document/d/1Hh_NQXo6IsRkgZaHeAEKmcDWRZXIDQYvLUKaRyVvk6IQ/edit?usp=sharing

(cherry picked from commit [f84c79a85f49295be97af1a3dc021c333710501d](https://chromium-review.googlesource.com/c/chromium/src/+2840903))

Bug-1478203

Change-Id: I5e1a83d68b521db33118ba74e98b8565b02ae6eb
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2840903>
Commit-Queue: Max Curran <curranmax@chromium.org>
Reviewed-by: Robert Ogden <robertogden@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#876861}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2875639>
Auto-Submit: Max Curran <curranmax@chromium.org>
Reviewed-by: Tarun Bansal <tbansal@chromium.org>
Commit-Queue: Tarun Bansal <tbansal@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1409}
Cr-Branched-From: e5ce7dc47518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] <https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/browser/BUILD.gn>
[modify] https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/browser/chrome_content_browser_client.cc
[add] https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/browser/offline_pages/offline_page_navigation_throttle.cc
[add] https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/browser/offline_pages/offline_page_navigation_throttle.h
[add] https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/browser/offline_pages/offline_page_navigation_throttle_unittest.cc
[modify] <https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/chrome/test/BUILD.gn>
[modify] https://crrev.com/3561caa4e0546a2968ade20e2c86ef48080845da/tools/metrics/histograms/histograms_xml/offline/histograms.xml

Comment 28 by [sheriffbot](#) on Thu, May 6, 2021, 2:02 PM EDT Project Member

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

Comment 29 by [Git Watcher](#) on Thu, May 6, 2021, 6:48 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/+9b78d81535e1158813996a163c61aa3c05e22962>

commit [9b78d81535e1158813996a163c61aa3c05e22962](#)

Author: Max Curran <curranmax@chromium.org>

Date: Thu May 06 22:47:05 2021

Cancels requests from the renderer with the X-Chrome-offline header.

This CL adds a OfflinePageNavigationThrottle which catches any renderer initiated requests that include the "X-Chrome-offline" header, and then cancels these requests. There is no legitimate reason for a renderer to make a request with this header, but a compromised renderer could add this header in order to read an arbitrary file.

Doc with more details: https://docs.google.com/document/d/1Hh_NQXo6IsRkgZaHeAEKmcDWRZXiDQYvLUKaRyVvK6iQ/edit?usp=sharing

(cherry picked from commit [f84c79a85f49295be97af1a3dc021c33710501d](#))

[Bug-1176303](#)

Change-Id: I5e1a83d68b521db33118ba74e98b8565b02ae6eb

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2840903>

Commit-Queue: Max Curran <curranmax@chromium.org>

Reviewed-by: Robert Ogden <robertogden@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#876861}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2875642>

Auto-Submit: Max Curran <curranmax@chromium.org>

Reviewed-by: Tarun Bansal <tbansal@chromium.org>

Commit-Queue: Tarun Bansal <tbansal@chromium.org>

Cr-Commit-Position: refs/branch-heads/4472@{#810}

Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] <https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/browser/BUILD.gn>
[modify] https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/browser/chrome_content_browser_client.cc
[add] https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/browser/offline_pages/offline_page_navigation_throttle.cc
[add] https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/browser/offline_pages/offline_page_navigation_throttle.h
[add] https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/browser/offline_pages/offline_page_navigation_throttle_unittest.cc
[modify] <https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/chrome/test/BUILD.gn>
[modify] https://crrev.com/9b78d81535e1158813996a163c61aa3c05e22962/tools/metrics/histograms/histograms_xml/offline/histograms.xml

Comment 30 by amyressler@chromium.org on Fri, May 7, 2021, 5:35 PM EDT Project Member

Labels: Release-3-M90

Comment 31 by vsavu@google.com on Mon, May 10, 2021, 9:13 AM EDT Project Member

Labels: LTS-Merge-Request-86

Comment 32 by vsavu@google.com on Mon, May 10, 2021, 9:13 AM EDT Project Member

Labels: LTS-Security-86

Comment 33 by amyressler@google.com on Mon, May 10, 2021, 9:53 AM EDT Project Member

Labels: CVE-2021-30507 CVE_description-missing

Comment 34 by gianluca@google.com on Wed, May 12, 2021, 12:34 PM EDT Project Member

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

Comment 35 by [Git Watcher](#) on Wed, May 12, 2021, 12:51 PM EDT Project Member

Labels: merge-merged-4240

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+75445e97fd32726ed264af922cf70f1ef595a815>

commit [75445e97fd32726ed264af922cf70f1ef595a815](#)

Author: Max Curran <curranmax@chromium.org>

Date: Wed May 12 16:50:04 2021

[M86-LTS]: Cancels requests from the renderer with the X-Chrome-offline header.

This CL adds a OfflinePageNavigationThrottle which catches any renderer initiated requests that include the "X-Chrome-offline" header, and then cancels these requests. There is no legitimate reason for a renderer to make a request with this header, but a compromised renderer could add this header in order to read an arbitrary file.

Doc with more details: https://docs.google.com/document/d/1Hh_NQXo6IsRkgZaHeAEKmcDWRZXiDQYvLUKaRyVvK6iQ/edit?usp=sharing

[M86]: Histogram change moved to correct file.

Minor conflicts resolved.

(cherry picked from commit [f84c79a85f49295be97af1a3dc021c333710501d](#))

[Bug-4478209](#)

Change-Id: I5e1a83d68b521db33118ba74e98b8565b02ae6eb
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2840903>
Commit-Queue: Max Curran <curranmax@chromium.org>
Reviewed-by: Robert Ogden <robertogden@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#876861}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2883702>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1633}
Cr-Branched-From: [f297677702651916bbf65e59c0d4bbd4ce57d1ee](#)-refs/heads/master@{#800218}

[modify] <https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/browser/BUILD.gn>
[modify] https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/browser/chrome_content_browser_client.cc
[add] https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/browser/offline_pages/offline_page_navigation_throttle.cc
[add] https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/browser/offline_pages/offline_page_navigation_throttle.h
[add] https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/browser/offline_pages/offline_page_navigation_throttle_unittest.cc
[modify] <https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/chrome/test/BUILD.gn>
[modify] <https://crrev.com/75445e97fd32726ed264af922cf70f1ef595a815/tools/metrics/histograms/histograms.xml>

[Comment 36](#) by [Git Watcher](#) on Thu, May 20, 2021, 7:02 AM EDT Project Member

Labels: merge-merged-4430_101

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+3e31693d503764879a1b2d51f36e394a4ef9c4dc>

commit [3e31693d503764879a1b2d51f36e394a4ef9c4dc](#)

Author: Max Curran <curranmax@chromium.org>

Date: Thu May 20 10:59:16 2021

Cancels requests from the renderer with the X-Chrome-offline header.

This CL adds a OfflinePageNavigationThrottle which catches any renderer initiated requests that include the "X-Chrome-offline" header, and then cancels these requests. There is no legitimate reason for a renderer to make a request with this header, but a compromised renderer could add this header in order to read an arbitrary file.

Doc with more details: https://docs.google.com/document/d/1Hh_NQXo6IsRkgZaHeAEKmcDWRZXIDQYvLUKaRyVv6iQ/edit?usp=sharing

(cherry picked from commit [f84c79a85f49295be97af1a3dc021c333710501d](#))

(cherry picked from commit [3561caa4e0546a2968ade20e2c86ef48080845da](#))

[Bug-4478209](#)

Change-Id: I5e1a83d68b521db33118ba74e98b8565b02ae6eb
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2840903>
Commit-Queue: Max Curran <curranmax@chromium.org>
Reviewed-by: Robert Ogden <robertogden@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#876861}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2875639>
Auto-Submit: Max Curran <curranmax@chromium.org>
Reviewed-by: Tarun Bansal <tbansal@chromium.org>
Commit-Queue: Tarun Bansal <tbansal@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1409}
Cr-Original-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@{#857950}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2884089>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430_101@{#41}
Cr-Branched-From: [3e9034a21f4b1f6707146b1309e001c3321ab48a](#)-refs/branch-heads/4430@{#1364}
Cr-Branched-From: [e5ce7dc4f7518237b3d9bb93cccca35d25216cbe](#)-refs/heads/master@{#857950}

[modify] <https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/browser/BUILD.gn>
[modify] https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/browser/chrome_content_browser_client.cc
[add] https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/browser/offline_pages/offline_page_navigation_throttle.cc
[add] https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/browser/offline_pages/offline_page_navigation_throttle.h
[add] https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/browser/offline_pages/offline_page_navigation_throttle_unittest.cc
[modify] <https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/chrome/test/BUILD.gn>
[modify] https://crrev.com/3e31693d503764879a1b2d51f36e394a4ef9c4dc/tools/metrics/histograms/histograms_xml/offline/histograms.xml

[Comment 37](#) by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 38](#) by [sheriffbot](#) on Thu, Aug 26, 2021, 1:30 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