Starred by 4 users

Owner:	qin...@chromium.org
CC:	adetaylor@chromium.org shaktisahu@chromium.org xingliu@chromium.org amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Downloads
Modified:	Sep 21, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Android
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-3000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-91
Target-91
external_security_report
FoundIn-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
Release-0-M92
merge-merged-4577
merge-merged-93
CVE-2021-30584

Issue 1213350: Security: Incorrect Security UI in downloads

Reported by zyzen...@gmail.com on Wed, May 26, 2021, 4:03 AM EDT

Code

Steps to reproduce the problem:
Note: this is not a regression of ~~issue 1157743~~

1.host index.html at http://192.168.1.x, and then visit it in android chrome
```
<iframe srcdoc="<script>document.location='1.php'</script>"></iframe>
```

source code of 1.php
```
<?php
    header('Content-Description: File Transfer');
    header('Content-Type: text/plain');
    header('Content-Disposition: attachment; filename="test"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: 13400');
    echo "xxxxxxxxxx";
?>
```
2.after download, please check your download lists in settings

3.chrome thinks this file "test.txt" is downloaded from about:srcdoc instead of its real address http://192.168.1.x

What is the expected behavior?
show http://192.168.1.x

What went wrong?
show a wrong address about:srcdoc

Did this work before? N/A

Chrome version: 93.0.4522.0 Channel: canary
OS Version: 11
Flash Version:

[Deleted] **dl_spoof.jpg**

Comment 1 by sheriffbot on Wed, May 26, 2021, 4:07 AM EDT Project Member

Labels: external_security_report

Comment 2 by adetaylor@google.com on Wed, May 26, 2021, 5:17 PM EDT Project Member

Owner: qin...@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium
Components: UI>Browser>Downloads

Reproduced on Chrome 91.0.4472.77 using the following files:

xxx - just a blank file
index.html - exactly as specified in #c0
silly.py:

====
```
#!/usr/bin/env python

# Attribution: https://stackoverflow.com/questions/21956683/enable-access-control-on-simple-http-server

try:
    # Python 3
    from http.server import HTTPServer, SimpleHTTPRequestHandler, test as test_orig
    import sys
    def test (*args):
        test_orig(*args, port=int(sys.argv[1]) if len(sys.argv) > 1 else 8000)
except ImportError: # Python 2
    from BaseHTTPServer import HTTPServer, test
    from SimpleHTTPServer import SimpleHTTPRequestHandler

class CORSRequestHandler (SimpleHTTPRequestHandler):
    def end_headers (self):
        if 'xxx' in self.path:
            self.send_header('Access-Control-Allow-Origin', '*')
            self.send_header('Content-Description', 'File Transfer');
            self.send_header('Content-Type', 'text/plain');
            self.send_header('Content-Disposition', 'attachment; filename="test"');
            self.send_header('Expires','0');
            self.send_header('Cache-Control','must-revalidate');
            self.send_header('Pragma','public');
        SimpleHTTPRequestHandler.end_headers(self)

if __name__ == '__main__':
    test(CORSRequestHandler, HTTPServer)
```
====

python3 silly.py then just connect to it.

Severity guidelines say that a URL spoof "where only certain URLs can be displayed, or with other mitigating factors" is medium.

It doesn't seem to do the same in the desktop download list.

Comment 3 by sheriffbot on Thu, May 27, 2021, 1:04 PM EDT Project Member

Labels: M-91 Target-91

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 4 by sheriffbot on Thu, May 27, 2021, 1:40 PM EDT Project Member

Labels: -Pri-2 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 5 by sheriffbot on Thu, May 27, 2021, 2:39 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 6 by qin...@chromium.org on Thu, May 27, 2021, 2:53 PM EDT Project Member

Cc: xingliu@chromium.org shaktisahu@chromium.org

Comment 7 by Git Watcher on Tue, Jun 1, 2021, 11:37 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0

commit e6039c6dad7d380f0d7c0866cb29f0bc4a589da0
Author: Min Qin <qinmin@chromium.org>
Date: Tue Jun 01 15:36:48 2021

Use url instead of pageUrl in OfflineItem

This page url is very confusing. In DownloadItem.java, page url is
from a download's URL, while in offline_item_utils.cc, page url is
from the tab URL.
Since page url is never used anywhere other than download home
previously, and download home is also not using it anymore,
this CL replaces the page URL with the URL of the download item.
This CL also started to use a download's URL for display on download
home, rather than the original URL. This will make Android download
URL display to match the behavior on that of the desktop.
Our previous discussion in https://chromium-review.googlesource.com/c/chromium/src/+/2827403/2
prefers original URL. But since original URL can be a
script, so a wrong about:srcdoc is shown instead. Using URL of
the download will avoid this issue, though user might get confused
a download from A.com will show B.com if there is a redirect.

~~BUG=1213350~~

Change-Id: Id30b249c65d306c78af2e3f21d5ce94940540af6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2921772
Reviewed-by: Xing Liu <xingliu@chromium.org>
Reviewed-by: Scott Little <sclittle@chromium.org>
Reviewed-by: Rayan Kanso <rayankans@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>

Cr-Commit-Position: refs/heads/master@{#887981}

[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/android/java/src/org/chromium/chrome/browser/download/DownloadItem.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/background_fetch/background_fetch_browsertest.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/content_index/content_index_provider_impl.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/content_index/content_index_provider_unittest.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/android/java/src/org/chromium/chrome/browser/download/DownloadInfo.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/StubbedProvider.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/DateOrderedListMutatorTest.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/ShareUtils.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/ShareUtilsTest.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/UiUtils.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/mutator/GroupCardLabelAdder.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/offline_item_model.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/offline_item_utils.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/download/offline_item_utils_unittest.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/chrome/browser/offline_pages/android/downloads/offline_page_download_bridge.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/android/java/src/org/chromium/components/offline_items_collection/OfflineItem.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/android/java/src/org/chromium/components/offline_items_collection/bridges/OfflineItemBridge.java
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/android/offline_item_bridge.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/offline_item.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/offline_item.h
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_items_collection/core/test_support/offline_item_test_support.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_pages/core/downloads/download_ui_adapter_unittest.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_pages/core/downloads/offline_item_conversions.cc
[modify] https://crrev.com/e6039c6dad7d380f0d7c0866cb29f0bc4a589da0/components/offline_pages/core/downloads/offline_item_conversions_unittest.cc

Comment 8 by adetaylor@google.com on Tue, Jun 1, 2021, 8:39 PM EDT Project Member

Labels: FoundIn-91

Comment 9 by sheriffbot on Fri, Jun 11, 2021, 12:21 PM EDT Project Member

qinmin: 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 10 by qin...@chromium.org on Fri, Jun 11, 2021, 12:24 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 11 by sheriffbot on Fri, Jun 11, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 12 by sheriffbot on Fri, Jun 11, 2021, 2:03 PM EDT Project Member

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

Comment 13 by sheriffbot on Fri, Jun 11, 2021, 2:28 PM EDT Project Member

Labels: Merge-Request-92

Requesting merge to beta M92 because latest trunk commit (887981) appears to be after beta branch point (885287).

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

Comment 14 by sheriffbot on Fri, Jun 11, 2021, 2:32 PM EDT Project Member

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

This bug requires manual review: M92'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: govind@(Android), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 15 by gov...@chromium.org on Fri, Jun 11, 2021, 3:08 PM EDT Project Member

Cc: adetaylor@chromium.org amyressler@chromium.org

+Security TPMS for M92 merge review. Thank you.

Comment 16 by amyressler@chromium.org on Mon, Jun 14, 2021, 10:05 AM EDT Project Member

Labels: -Merge-Review-92 Merge-Approved-92

this is a rather large change for medium severity bug, but given it has been on Canary for almost two weeks now, approving for beta/M92 merge, please merge to branch 4515

Comment 17 by gov...@chromium.org on Mon, Jun 14, 2021, 12:47 PM EDT Project Member

Please merge your change to M92 branch 4515 ASAP so we can take it in for this week Beta release. Thank you.

Comment 18 by Git Watcher on Mon, Jun 14, 2021, 11:21 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/+/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f

commit 7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f
Author: Min Qin <qinmin@chromium.org>
Date: Tue Jun 15 03:20:24 2021

Use url instead of pageUrl in OfflineItem

This page url is very confusing. In DownloadItem.java, page url is
from a download's URL, while in offline_item_utils.cc, page url is
from the tab URL.
Since page url is never used anywhere other than download home
previously, and download home is also not using it anymore,
this CL replaces the page URL with the URL of the download item.
This CL also started to use a download's URL for display on download
home, rather than the original URL. This will make Android download
URL display to match the behavior on that of the desktop.
Our previous discussion in https://chromium-review.googlesource.com/c/chromium/src/+/2827403/2
prefers original URL. But since original URL can be a
script, so a wrong about:srcdoc is shown instead. Using URL of
the download will avoid this issue, though user might get confused
a download from A.com will show B.com if there is a redirect.

~~BUG=1213350~~

(cherry picked from commit e6039c6dad7d380f0d7c0866cb29f0bc4a589da0)

Change-Id: Id30b249c65d306c78af2e3f21d5ce94940540af6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2921772
Reviewed-by: Xing Liu <xingliu@chromium.org>
Reviewed-by: Scott Little <sclittle@chromium.org>
Reviewed-by: Rayan Kanso <rayankans@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#887981}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2961173
Cr-Commit-Position: refs/branch-heads/4515@{#607}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/android/java/src/org/chromium/chrome/browser/download/DownloadItem.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/background_fetch/background_fetch_browsertest.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/content_index/content_index_provider_impl.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/content_index/content_index_provider_unittest.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/android/java/src/org/chromium/chrome/browser/download/DownloadInfo.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/StubbedProvider.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/DateOrderedListMutatorTest.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/ShareUtils.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/ShareUtilsTest.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/UiUtils.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/internal/android/java/src/org/chromium/chrome/browser/download/home/list/mutator/GroupCardLabelAdder.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/offline_item_model.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/offline_item_utils.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/download/offline_item_utils_unittest.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/chrome/browser/offline_pages/android/downloads/offline_page_download_bridge.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/android/java/src/org/chromium/components/offline_items_collection/OfflineItem.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/android/java/src/org/chromium/components/offline_items_collection/bridges/OfflineItemBridge.java
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/android/offline_item_bridge.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/offline_item.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/offline_item.h
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_items_collection/core/test_support/offline_item_test_support.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_pages/core/downloads/download_ui_adapter_unittest.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_pages/core/downloads/offline_item_conversions.cc
[modify] https://crrev.com/7e8ce4c0761bbbfdf629a5b33bdb6de9ceab392f/components/offline_pages/core/downloads/offline_item_conversions_unittest.cc

Comment 19 by amyressler@google.com on Wed, Jun 23, 2021, 7:24 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 20 by amyressler@chromium.org on Wed, Jun 23, 2021, 7:45 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $3,000 for this report. Nice work!

Comment 21 by amyressler@google.com on Wed, Jun 30, 2021, 5:35 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 22 by amyressler@chromium.org on Mon, Jul 19, 2021, 3:10 PM EDT Project Member

Labels: Release-0-M92

Comment 23 by amyressler@google.com on Mon, Jul 19, 2021, 7:18 PM EDT Project Member

Labels: CVE-2021-30584 CVE_description-missing

Comment 24 by rzanoni@google.com on Tue, Jul 27, 2021, 9:40 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merged-90

Comment 25 by Git Watcher on Thu, Jul 29, 2021, 5:59 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7bec935d94d00ebca571b838bf593d337aac4397

commit 7bec935d94d00ebca571b838bf593d337aac4397
Author: Xing Liu <xingliu@chromium.org>
Date: Thu Jul 29 21:58:24 2021

Download: Fix final URL plumbing for old download code path.

When UseDownloadOfflineContentProvider feature is disabled, the URL
shown on the UI is still tab URL, this CL fixed the plumbing to improve
security for the old code path.

~~Bug: 1198165,1213350~~
Change-Id: I6e8940491e3030b8c70b1058c955d0fdc8d01e3d
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3061420
Reviewed-by: Min Qin <qinmin@chromium.org>
Commit-Queue: Xing Liu <xingliu@chromium.org>
Cr-Commit-Position: refs/heads/master@{#906866}

[modify] https://crrev.com/7bec935d94d00ebca571b838bf593d337aac4397/chrome/browser/download/android/download_manager_service.cc

Comment 26 by amyressler@google.com on Tue, Aug 3, 2021, 3:42 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 27 by Git Watcher on Wed, Aug 4, 2021, 5:06 PM EDT Project Member

Labels: merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/86a9684977f0e5869d3b7a9f8f48f17c893ff52f

commit 86a9684977f0e5869d3b7a9f8f48f17c893ff52f
Author: Xing Liu <xingliu@chromium.org>
Date: Wed Aug 04 21:05:00 2021

Download: Fix final URL plumbing for old download code path.

When UseDownloadOfflineContentProvider feature is disabled, the URL
shown on the UI is still tab URL, this CL fixed the plumbing to improve
security for the old code path.

(cherry picked from commit 7bec935d94d00ebca571b838bf593d337aac4397)

~~Bug: 1198165,1213350~~
Change-Id: I6e8940491e3030b8c70b1058c955d0fdc8d01e3d
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3061420
Reviewed-by: Min Qin <qinmin@chromium.org>
Commit-Queue: Xing Liu <xingliu@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#906866}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3072318
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4577@{#448}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/86a9684977f0e5869d3b7a9f8f48f17c893ff52f/chrome/browser/download/android/download_manager_service.cc

Comment 28 by sheriffbot on Tue, Sep 21, 2021, 1:31 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