Starred by 4 users

Owner:	thestig@chromium.org
CC:	adetaylor@google.com j...@igalia.com
Status:	Fixed *(Closed)*
Components:	Internals>Printing
Modified:	Sep 11, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

reward-10000
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
Merge-Rejected-90
M-92
Target-92
external_security_report
merge-merged-4430
merge-merged-90
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
Release-0-M92
CVE-2021-30566
LTS-Size-Small
LTS-Complexity-Minimal

Issue 1202661: Security: Stack overflow in printing

Reported by leecraso@gmail.com on Mon, Apr 26, 2021, 7:27 AM EDT

Code

VULNERABILITY DETAILS
Another example of the bugs same as ~~crbug.com/1138143~~ and ~~crbug.com/1202643~~. IPC-call |PrintingFailed|[1] could recursively create nested message loops[2]. Frequent calling of it will eventually lead to the stack overflow.

[1]. https://source.chromium.org/chromium/chromium/src/+/master:components/printing/common/print.mojom;l=361;drc=7f5777c93e60f6ea177b9ff69e4cd4e1d5d0af19
[2]. https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/printing/print_error_dialog.cc;l=20;bpv=1;bpt=0;drc=b2bbd48743b3df3de037c1633e7ca658f08e7469

VERSION
Chrome Version: stable
Operating System: All

REPRODUCTION CASE

1. Apply the attached patch.diff to emulates a compromised renderer.
2. $ python ./copy_mojo_js_bindings.py /path/to/chrome/.../out/asan/gen
   $ python -m SimpleHTTPServer
   $ out/asan/chrome --user-data-dir=/tmp/xxxx "http://localhost:8000/poc.html"

Wait for around 30s, you will get a segmentation fault.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: browser
Crash State: see attached debug_info file

CREDIT INFORMATION
Reporter credit: Leecraso and Guang Gong of 360 Alpha Lab

patch.diff
810 bytes View Download

debug_info.txt
7.8 KB View Download

poc.html
32 bytes View Download

Comment 1 by sheriffbot on Mon, Apr 26, 2021, 7:29 AM EDT Project Member

Labels: external_security_report

Comment 2 by carlosil@chromium.org on Mon, Apr 26, 2021, 8:58 PM EDT Project Member

Owner: rbpotter@chromium.org
Cc: j...@igalia.com
Labels: Security_Severity-High Security_Impact-Stable OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Internals>Printing

Assigning high severity since this needs a compromised renderer.

rbpotter: Can you help further triage this? Thanks
jkim: cc'd since you've been working around the relevant code

Comment 3 by thestig@chromium.org on Mon, Apr 26, 2021, 9:04 PM EDT Project Member

Owner: thestig@chromium.org

To be clear, which process will suffer from stack overflow? The browser process or a renderer?

Comment 4 by leecraso@gmail.com on Mon, Apr 26, 2021, 10:09 PM EDT

Thanks for the quick reply. It is a crash of the browser process.

Comment 5 by leecraso@gmail.com on Mon, Apr 26, 2021, 11:21 PM EDT

Just in case someone doesn't have permission to view ~~crbug.com/1202612~~. I'm here to quote some of the content in it that may be helpful.

>> Same as ~~crbug.com/1138143~~, there are many other modules that could create nested message loops[1]. If we call those functions frequently to create nested message loops recursively, the stack will be pushed constantly, and eventually leading to the stack overflow as ~~crbug.com/1138143~~. The details are as I said in ~~crbug.com/1138143#c70~~.

[1]. https://source.chromium.org/chromium/chromium/src/+/master:base/run_loop.cc;l=111;bpv=1;bpt=0;drc=e125e8d6661068afe340b0fd2c09d49f74ffe48b

Comment 6 by sheriffbot on Tue, Apr 27, 2021, 12:48 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 7 by sheriffbot on Tue, Apr 27, 2021, 1:28 PM EDT Project Member

Labels: -Pri-3 Pri-1

Setting Pri-1 to match security severity High. 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 8 by sheriffbot on Tue, Apr 27, 2021, 2:38 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 9 by leecraso@gmail.com on Thu, Apr 29, 2021, 9:19 PM EDT

friendly ping

Comment 10 by thestig@chromium.org on Fri, Apr 30, 2021, 12:18 AM EDT Project Member

Pong. Isn't this mostly a denial of service attack where a compromised renderer can crash the browser?

Comment 11 by leecraso@gmail.com on Fri, Apr 30, 2021, 1:57 AM EDT

Actually, same as ~~crbug.com/1138143~~, I think it's a memory corruption issue that could be exploited. The address it visits is not a null pointer or illegal address, but the space above the stack with an offset. If the attacker could allocate the space above the stack, he can do the stack pivot with controllable data.

Comment 12 by leecraso@gmail.com on Thu, May 6, 2021, 5:55 AM EDT

Hi, any updates?

Comment 13 by leecraso@gmail.com on Thu, May 6, 2021, 11:25 PM EDT

I think this bug can be fixed by using a static flag like [1].

[1].
https://source.chromium.org/chromium/chromium/src/+/master:chrome/browser/printing/print_view_manager_base.cc;l=79;drc=dec9912407fc5946125799ec62b996a04d08c4f0

Comment 14 by leecraso@gmail.com on Thu, May 6, 2021, 11:30 PM EDT

suggestion.diff
709 bytes View Download

Comment 15 by Git Watcher on Mon, May 10, 2021, 3:02 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3e988ae0aebf9f60b578aefa71168f76aaeaa686

commit 3e988ae0aebf9f60b578aefa71168f76aaeaa686
Author: Lei Zhang <thestig@chromium.org>
Date: Mon May 10 19:01:53 2021

Check cookie in PrintViewManagerBase::PrintingFailed().

This check got lost in https://crrev.com/338697 when parts of
PrintViewManagerBase split off into PrintManager.

~~Bug: 1202661~~
Change-Id: I85d481912d6300296d5c186d3e8d834050de3097
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2881382
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Commit-Position: refs/heads/master@{#881135}

[modify] https://crrev.com/3e988ae0aebf9f60b578aefa71168f76aaeaa686/chrome/browser/printing/print_view_manager_base.cc
[modify] https://crrev.com/3e988ae0aebf9f60b578aefa71168f76aaeaa686/components/printing/browser/print_manager.cc
[modify] https://crrev.com/3e988ae0aebf9f60b578aefa71168f76aaeaa686/components/printing/browser/print_manager.h

Comment 16 by thestig@chromium.org on Mon, May 10, 2021, 3:06 PM EDT Project Member

Status: Fixed (was: Assigned)

Thanks for the suggestion, but it is better to fix the root problem that allows the renderer to spam "printing failed" IPC calls.

Comment 17 by leecraso@gmail.com on Mon, May 10, 2021, 10:55 PM EDT

Hi thestig@, thanks for the reply, but it seems the |cookie_| could also be set[1] through IPC call |DidGetDocumentCookie|[2].

[1]. https://source.chromium.org/chromium/chromium/src/+/main:components/printing/browser/print_manager.cc;l=33;drc=3e988ae0aebf9f60b578aefa71168f76aaeaa686
[2]. https://source.chromium.org/chromium/chromium/src/+/main:components/printing/common/print.mojom;l=326;drc=3e988ae0aebf9f60b578aefa71168f76aaeaa686

Comment 18 by thestig@chromium.org on Tue, May 11, 2021, 3:04 AM EDT Project Member

Status: Started (was: Fixed)

re: comment 17: Sure. I'll take care of that next.

Comment 19 by Git Watcher on Mon, May 24, 2021, 3:28 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/eead1ba5da342d167728bf9c3d2d156661e312a8

commit eead1ba5da342d167728bf9c3d2d156661e312a8
Author: Lei Zhang <thestig@chromium.org>
Date: Mon May 24 19:27:31 2021

Remove PrintManagerHost::DidGetDocumentCookie() interface.

In PrintManager and derived classes, set the document cookie used for
printing in those classes in the browser process. Don't pass it to a
renderer, get the value back, and then set it.

~~Bug: 1202661~~
Change-Id: I9482c886d7aa3d2e17f06d8d218f87f8e27784f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2909373
Reviewed-by: Alan Screen <awscreen@chromium.org>
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Commit-Position: refs/heads/master@{#886032}

[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/chrome/browser/printing/print_view_manager_base.cc
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/chrome/browser/printing/print_view_manager_base.h
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/components/printing/browser/print_manager.cc
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/components/printing/browser/print_manager.h
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/components/printing/common/print.mojom
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/components/printing/test/print_render_frame_helper_browsertest.cc
[modify] https://crrev.com/eead1ba5da342d167728bf9c3d2d156661e312a8/headless/lib/browser/headless_print_manager.cc

Comment 20 by thestig@chromium.org on Mon, May 24, 2021, 3:50 PM EDT Project Member

Status: Fixed (was: Started)

Comment 21 by sheriffbot on Tue, May 25, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 22 by sheriffbot on Tue, May 25, 2021, 2:03 PM EDT Project Member

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

Comment 23 by sheriffbot on Tue, May 25, 2021, 2:24 PM EDT Project Member

Labels: Merge-Request-92 Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (886032) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (886032) appears to be after beta branch point (870763).

Requesting merge to future beta M92 because latest trunk commit (886032) appears to be after future beta branch point (884198).

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

Comment 24 by sheriffbot on Tue, May 25, 2021, 2:27 PM EDT Project Member

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

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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 25 by thestig@chromium.org on Tue, May 25, 2021, 3:07 PM EDT Project Member

We probably should let r886032 bake on Dev/Canary channel for a bit before merging.

Comment 26 by sheriffbot on Wed, May 26, 2021, 12:22 PM EDT Project Member

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

Comment 27 by sheriffbot on Wed, May 26, 2021, 2:27 PM EDT Project Member

Labels: -Merge-Request-92 Hotlist-Merge-Approved Merge-Approved-92

Your change meets the bar and is auto-approved for M92. Please go ahead and merge the CL to branch 4515 (refs/branch-heads/4515) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: govind@(Android), bindusuvarna@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 28 by srinivassista@google.com on Thu, May 27, 2021, 2:02 PM EDT Project Member

Labels: -Target-90 -Merge-Request-90 Merge-Rejected-90

Rejecting the merge for M90 and dropping 90 labels.

Comment 29 by sheriffbot on Mon, May 31, 2021, 12:17 PM EDT Project Member

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 30 by gov...@chromium.org on Tue, Jun 1, 2021, 3:23 PM EDT Project Member

Please merge your change to M92 branch 4515 ASAP. Thank you.

Comment 31 by gov...@chromium.org on Wed, Jun 2, 2021, 12:53 PM EDT Project Member

Please merge your change to M92 branch 4515 ASAP. Thank you.

Comment 32 by amyressler@google.com on Wed, Jun 2, 2021, 3:51 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 33 by amyressler@chromium.org on Thu, Jun 3, 2021, 12:18 PM EDT Project Member

Congratulations, leecraso! The VRP Panel has decided to award you $10,000 for this report. Nice work.

Comment 34 by amyressler@chromium.org on Thu, Jun 3, 2021, 12:32 PM EDT Project Member

Hi leecraso, to respond to your questions about the reward amount: the panel decided this reward amount based on the full context of the bug and bug report.
In analyzing the bug and this report, the exploitability was not demonstrated and more theoretical, as per comments 10-11.

As it's "a memory corruption issue that could be exploited", but was not demonstrated as such, the Panel has decided on this reward amount accordingly. Thanks!

Comment 35 by adetaylor@google.com on Thu, Jun 3, 2021, 2:34 PM EDT Project Member

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

thestig@

Approving merge to M91, branch 4472. We're making a security refresh tomorrow, so please go ahead and merge. However I note your comment in #c25 that this needs bake time... if you think it's too soon to merge, it's OK to avoid merging right now.

Comment 36 by pbommana@google.com on Thu, Jun 3, 2021, 3:33 PM EDT Project Member

Your change has been approved for M91. Please go ahead and merge the CL to M91 branch : 4472 (refs/branch-heads/4472) manually asap.

Comment 37 by gov...@chromium.org on Fri, Jun 4, 2021, 1:53 AM EDT Project Member

Please merge your change to M92 branch 4515 ASAP. Thank you.

Comment 38 by thestig@chromium.org on Fri, Jun 4, 2021, 4:35 AM EDT Project Member

re: comment 35 / comment 36 - I still want to let this bake more, so skipping M91 for now. Will merge to M92. Given this issue has been around for ~10 years, I think we can hold off for 1 more milestone?

Comment 39 by amyressler@google.com on Fri, Jun 4, 2021, 10:45 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 40 by Git Watcher on Fri, Jun 4, 2021, 3:08 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/+/21c0a3d2f45de0c1eadef657749323f02c8e9799

commit 21c0a3d2f45de0c1eadef657749323f02c8e9799
Author: Lei Zhang <thestig@chromium.org>
Date: Fri Jun 04 19:07:32 2021

M92: Remove PrintManagerHost::DidGetDocumentCookie() interface.

In PrintManager and derived classes, set the document cookie used for
printing in those classes in the browser process. Don't pass it to a
renderer, get the value back, and then set it.

(cherry picked from commit eead1ba5da342d167728bf9c3d2d156661e312a8)

~~Bug: 1202661~~
Change-Id: I9482c886d7aa3d2e17f06d8d218f87f8e27784f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2909373
Reviewed-by: Alan Screen <awscreen@chromium.org>
Reviewed-by: Robert Sesek <rsesek@chromium.org>
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#886032}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2940003
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4515@{#330}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/chrome/browser/printing/print_view_manager_base.cc
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/chrome/browser/printing/print_view_manager_base.h

[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/components/printing/browser/print_manager.cc
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/components/printing/browser/print_manager.h
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/components/printing/common/print.mojom
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/components/printing/test/print_render_frame_helper_browsertest.cc
[modify] https://crrev.com/21c0a3d2f45de0c1eadef657749323f02c8e9799/headless/lib/browser/headless_print_manager.cc

Comment 41 by sheriffbot on Mon, Jun 7, 2021, 12:17 PM EDT Project Member

Cc: adetaylor@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 42 by thestig@chromium.org on Mon, Jun 7, 2021, 2:35 PM EDT Project Member

Labels: -Hotlist-Merge-Review -Hotlist-Merge-Approved -M-91 -Merge-Approved-91 -Target-91 M-92 Target-92

Comment 43 by amyressler@chromium.org on Mon, Jul 19, 2021, 4:16 PM EDT Project Member

Labels: Release-0-M92

Comment 44 by amyressler@google.com on Mon, Jul 19, 2021, 7:14 PM EDT Project Member

Labels: CVE-2021-30566 CVE_description-missing

Comment 45 by rzanoni@google.com on Fri, Jul 30, 2021, 3:52 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 46 by amyressler@google.com on Tue, Aug 3, 2021, 3:41 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 47 by gianluca@google.com on Thu, Aug 5, 2021, 6:24 AM EDT Project Member

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

Comment 48 by Git Watcher on Thu, Aug 5, 2021, 9:18 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7b000516582f48869794f82f9be5da8f89fe4fee

commit 7b000516582f48869794f82f9be5da8f89fe4fee
Author: Lei Zhang <thestig@chromium.org>
Date: Thu Aug 05 13:17:20 2021

[M90-LTS] Check cookie in PrintViewManagerBase::PrintingFailed().

This check got lost in https://crrev.com/338697 when parts of
PrintViewManagerBase split off into PrintManager.

(cherry picked from commit 3e988ae0aebf9f60b578aefa71168f76aaeaa686)

~~Bug: 1202661~~
Change-Id: I85d481912d6300296d5c186d3e8d834050de3097
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2881382
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#881135}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3060063
Reviewed-by: Jana Grill <janagrill@google.com>
Owners-Override: Jana Grill <janagrill@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1552}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/7b000516582f48869794f82f9be5da8f89fe4fee/chrome/browser/printing/print_view_manager_base.cc
[modify] https://crrev.com/7b000516582f48869794f82f9be5da8f89fe4fee/components/printing/browser/print_manager.cc
[modify] https://crrev.com/7b000516582f48869794f82f9be5da8f89fe4fee/components/printing/browser/print_manager.h

Comment 49 by Git Watcher on Thu, Aug 5, 2021, 10:10 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/56ba41ba1b3129579fc06ada5a2a9f85a34f994e

commit 56ba41ba1b3129579fc06ada5a2a9f85a34f994e
Author: Lei Zhang <thestig@chromium.org>
Date: Thu Aug 05 14:07:08 2021

[M90-LTS] Remove PrintManagerHost::DidGetDocumentCookie() interface.

In PrintManager and derived classes, set the document cookie used for
printing in those classes in the browser process. Don't pass it to a
renderer, get the value back, and then set it.

(cherry picked from commit eead1ba5da342d167728bf9c3d2d156661e312a8)

~~Bug: 1202661~~
Change-Id: I9482c886d7aa3d2e17f06d8d218f87f8e27784f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2909373
Commit-Queue: Lei Zhang <thestig@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#886032}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3060066
Reviewed-by: Jana Grill <janagrill@google.com>
Owners-Override: Jana Grill <janagrill@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1558}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/chrome/browser/printing/print_view_manager_base.cc
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/chrome/browser/printing/print_view_manager_base.h

[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/components/printing/browser/print_manager.cc
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/components/printing/browser/print_manager.h
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/components/printing/common/print.mojom
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/components/printing/renderer/print_render_frame_helper.cc
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/components/printing/test/print_render_frame_helper_browsertest.cc
[modify] https://crrev.com/56ba41ba1b3129579fc06ada5a2a9f85a34f994e/headless/lib/browser/headless_print_manager.cc

Comment 50 by rzanoni@google.com on Thu, Aug 5, 2021, 10:12 AM EDT Project Member

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

Comment 51 by sheriffbot on Sat, Sep 11, 2021, 1:34 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