


☆ Starred by 3 users


Owner:

rbpott@chromium.org


CC:



 karandeepb@chromium.org  
adetaylor@chromium.org  
rdevl...@chromium.org  
thestig@chromium.org  
creis@chromium.org  



 zachbutler@google.com  
dcheng@chromium.org  
rbpott@chromium.org  



 nasko@chromium.org  
solomonkinard@chromium.org  
tjudkins@chromium.org  
wfh@chromium.org  
ajgo@chromium.org

Status:

Fixed (Closed)

Components:

Services>CloudPrint  
Internals>Sandbox>Sitelisolation  
Platform>Extensions

Modified:

Jun 24, 2021

Backlog-Rank:

----

Editors:

----

EstimatedDays:

----

NextAction:

----

OS:

Linux, Mac, Fuchsia

Pri:

2

Type:

Bug-Security

Reward-1000  
Security\_Severity-Low  
Security\_Impact-Stable  
allpublic  
reward-inprocess  
CVE\_description-submitted  
M-87  
Target-85  
Target-86  
Target-87  
Release-0-M89  
external\_security\_report  
CVE-2021-21185  
external\_security\_bug

Issue 1100748: Security: Possible for extensions to access chrome.cloudPrintPrivate API

Reported by derce...@gmail.com on Tue, Jun 30, 2020, 12:45 AM EDT

 Code

VULNERABILITY DETAILS

The Google Cloud Print site uses the chrome.cloudPrintPrivate API to retrieve a list of local printers and add them to the users account. This API is requested by the Cloud Print component extension and is granted to [https://www.google.com/cloudprint/enable\\_chrome\\_connector](https://www.google.com/cloudprint/enable_chrome_connector).

Therefore, any extension that has access to <https://www.google.com> can use the API.

VERSION

Chrome Version: Tested on 83.0.4103.116 (stable) and 86.0.4186.0 (canary)  
Operating System: Windows 10, version 1909

REPRODUCTION CASE

1. Install the attached extension.  
2. Once installed, the extension will open a new tab at the following location:  
  
[https://www.google.com/cloudprint/enable\\_chrome\\_connector](https://www.google.com/cloudprint/enable_chrome_connector)

3. As the extension requests hosts permissions for <https://www.google.com>, it's able to use chrome.tabs.executeScript to execute code within the context of this tab. Therefore, it makes the following call to log a list of printers to the console:

chrome.tabs.executeScript(targetTab.id, {code: "let script = document.createElement('script'); script.src = 'data:text/javascript,chrome.cloudPrintPrivate.getPrinters(function (printers) {console.log('Printers retrieved: ', printers)});'; document.head.appendChild(script);"});

CREDIT INFORMATION

Reporter credit: David Erceg

background.js

652 bytes [View](#) [Download](#)

manifest.json

243 bytes [View](#) [Download](#)

Comment 1 by derce...@gmail.com on Tue, Jun 30, 2020, 12:53 AM EDT

Overall, this issue has some similarity to [issue 927482](#), in that a private API can be accessed from other contexts.

One thing I've noticed is that [https://www.google.com/cloudprint/enable\\_chrome\\_connector](https://www.google.com/cloudprint/enable_chrome_connector) is isolated in a separate process. I believe that's due to the fact that the site instance URL is for the associated extension. That means other pages on the <https://www.google.com> origin can't script or access it in any way.

Additionally, an extension can't attach to the page using chrome.debugger.attach. That's because the request first goes through RenderFrameDevToolsAgentHost::ShouldAllowSession:

[https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/render\\_frame\\_devtools\\_agent\\_host.cc;lines=816;drc=df02f91d9c0548e4ea094f89ce2e293cd1f9083](https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/render_frame_devtools_agent_host.cc;lines=816;drc=df02f91d9c0548e4ea094f89ce2e293cd1f9083)

which returns:

```
session->GetClient()->MayAttachToURL(frame_host_->GetSiteInstance()->GetSiteURL(), frame_host_->web_ui())
```

In this case, `frame_host_->GetSiteInstance()->GetSiteURL()` returns:

`chrome-extension://mfhegcbipchphmccgaenjdiconmg/#https://google.com/`

This ultimately causes the request to be denied within `PermissionsData::IsRestrictedUri` because the current extension host doesn't match the site URL host:

[https://source.chromium.org/chromium/chromium/src/+master:extensions/common/permissions/permissions\\_data.cc;l=143;drc=efba8d2927574721d8e9c39c444a0c363694c312](https://source.chromium.org/chromium/chromium/src/+master:extensions/common/permissions/permissions_data.cc;l=143;drc=efba8d2927574721d8e9c39c444a0c363694c312)

On the other hand, `chrome.tabs.executeScript` will execute code on the page. The permission check is performed against the regular URL ([https://www.google.com/cloudprint/enable\\_chrome\\_connector](https://www.google.com/cloudprint/enable_chrome_connector)) and will succeed.

As far as I'm aware, the Web Store extension is the only other component extension that grants API functionality to a particular web URL (<https://chrome.google.com/webstore>). However, it's special-cased within `ChromeExtensionsClient::IsScriptableURL`:

[https://source.chromium.org/chromium/chromium/src/+master:chrome/common/extensions/chrome\\_extensions\\_client.cc;l=164;drc=d800f2cc8eb15c5a9be051c2abae15b145658a6](https://source.chromium.org/chromium/chromium/src/+master:chrome/common/extensions/chrome_extensions_client.cc;l=164;drc=d800f2cc8eb15c5a9be051c2abae15b145658a6)

That means that attempting to script <https://chrome.google.com/webstore> via `chrome.tabs.executeScript` will fail.

**Comment 2** by [carlosil@chromium.org](mailto:carlosil@chromium.org) on Tue, Jun 30, 2020, 3:37 PM EDT Project Member

**Status:** Assigned (was: Unconfirmed)

**Owner:** [rdevl...@chromium.org](mailto:rdevl...@chromium.org)

**Labels:** Security\_Impact-Stable Security\_Severity-Medium M-84 OS-Chrome OS-Fuchsia OS-Linux OS-Mac

**Components:** Platform>Extensions

Assigning medium severity to match the other [bug.com/937487](https://bug.com/937487) since this would also be mitigated by the extension install prompt listing the correct extensions.

Devlin: Can you help further triage and assign this? Thanks.

**Comment 3** by [rdevl...@chromium.org](mailto:rdevl...@chromium.org) on Tue, Jun 30, 2020, 4:02 PM EDT Project Member

**Owner:** [thestig@chromium.org](mailto:thestig@chromium.org)

**Cc:** [rdevl...@chromium.org](mailto:rdevl...@chromium.org) [creis@chromium.org](mailto:creis@chromium.org) [nasko@chromium.org](mailto:nasko@chromium.org)

Ooh, fun. Good find.

Hosted apps (excluding the webstore, which is very special in many ways) are basically web pages with a few more capabilities. They are designed to have relatively little power, and we've largely acknowledged that anything that can run in the context of the hosted app (i.e., in the context of the web page) can do the same things it can. This is normally fine, because hosted app privileges are usually pretty weak, and either extend or align with web permissions.

This is obviously an exception. On the upside, a quick search seems to indicate that this is the `_only_` exception - I don't see any other restricted APIs that are available to hosted apps (other than the webstore).

[thestig@chromium.org](mailto:thestig@chromium.org), do you know what the plan is for the cloudprint hosted app, since hosted apps are deprecated? Is there a plan in place to migrate it off? If so, what's the timeline like? If not, do you have other ideas how we could fix this?

My strong suspicion is that we don't want to make the same carveouts for cloudprint that we did for the webstore, but +nasko and creis FYI.

In the meantime, I'll see if we can also add a restriction against any more privileged APIs being exposed to hosted apps.

**Comment 4** by [thestig@chromium.org](mailto:thestig@chromium.org) on Tue, Jun 30, 2020, 4:30 PM EDT Project Member

We have no plans to migrate. Instead, Cloud Print as a whole is being shut down. The plan is to do that at the end of 2020, but the timeline may get extended a bit.

**Comment 5** by [thestig@chromium.org](mailto:thestig@chromium.org) on Wed, Jul 1, 2020, 2:54 AM EDT Project Member

**Labels:** -OS-Chrome

We can check that legitimate requests navigated from `chrome://devices`. Extensions can't navigate tabs to `chrome://` URLs, right?

**Comment 6** by [thestig@chromium.org](mailto:thestig@chromium.org) on Wed, Jul 1, 2020, 3:03 AM EDT Project Member

e.g. Something like <https://chromium-review.googlesource.com/2277106>

**Comment 7** by [sheriffbot](mailto:sheriffbot) on Wed, Jul 1, 2020, 2:47 PM EDT Project Member

**Labels:** 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 8** by [thestig@chromium.org](mailto:thestig@chromium.org) on Mon, Jul 6, 2020, 7:14 PM EDT Project Member

**Cc:** [dcheng@chromium.org](mailto:dcheng@chromium.org)

Still looking for some feedback on [comment 5](#) / [comment 6](#). Adding [dcheng@chromium.org](mailto:dcheng@chromium.org) for more eyeballs since all the folks CCed are busy.

**Comment 9** by [creis@chromium.org](mailto:creis@chromium.org) on Tue, Jul 7, 2020, 4:43 PM EDT Project Member

**Components:** Internals>Sandbox>Sitelisolation

**Comment 5:** Extensions with the `chrome.tabs` permission can navigate to `chrome://` URLs, right Devlin? The checks in [https://chromium-review.googlesource.com/c/chromium/src/+I2277106/1/chrome/browser/extensions/api/cloud\\_print\\_private/cloud\\_print\\_private\\_api.cc](https://chromium-review.googlesource.com/c/chromium/src/+I2277106/1/chrome/browser/extensions/api/cloud_print_private/cloud_print_private_api.cc) also seem a bit fragile, since the assumptions it makes about session history aren't always true. (e.g., 'You can't always assume that you can peek back one entry to see where the user came from-- that entry may have been cleared from browsing data, or because we hit the max number of entries, or overwritten with `location.replace`, etc.) Even if that worked, though, the extension would still have access to the API if the user went through the normal flow.

Devlin's right that content scripts are generally allowed to run within hosted apps, since those aren't supposed to be privileged. This API seems problematic since we aren't isolating the URL in any way. Indeed, we can't even isolate the origin as a special print endpoint since it's served from [www.google.com](https://www.google.com). It's unfortunate that Cloud Print depends on granting this API, and I'm glad it at least has a path to removal.

In the meantime, I do think we need to find a way to mitigate this. Is there any way to move the API to a different origin that we can isolate? Maybe even [chrome.google.com](https://chrome.google.com) to take advantage of the isolation added in [bug.com/939106](https://bug.com/939106)?

Alternatively, can the content script logic make an exception for this Cloud Print hosted app's URL(s) and prevent script injection there, until Cloud Print is removed?

**Comment 10** by [thestig@chromium.org](mailto:thestig@chromium.org) on Tue, Jul 7, 2020, 4:57 PM EDT Project Member

**Cc:** [zachbutler@google.com](mailto:zachbutler@google.com)

My CL is indeed fragile, but the only legit use, AFAIK, is from `chrome://devices`, where users navigate in the manner that my CL checks for.

+zachbutler to discuss server side options w.r.t. [comment 9](#).

**Comment 11** by [rdevl...@chromium.org](mailto:rdevl...@chromium.org) on Wed, Jul 8, 2020, 12:43 PM EDT Project Member

> Extensions with the chrome.tabs permission can navigate to chrome:// URLs, right Devlin?

In fact, even without the tabs permission. Any extension can create a tab to navigate to chrome://<anything>.

----

Note: I know nothing about how cloudprint works : )

> In the meantime, I do think we need to find a way to mitigate this. Is there any way to move the API to a different origin that we can isolate? Maybe even [chrome.google.com](#) to take advantage of the isolation added in [issue-536406](#)?

I think that'd be best - we'd get isolation + I think all of [chrome.google.com](#) is protected from script injection. I don't know how feasible this is, though, so interested to know from zachbutler@.

> Alternatively, can the content script logic make an exception for this Cloud Print hosted app's URL(s) and prevent script injection there, until Cloud Print is removed?

Theoretically - but this is ugly, and I'd really prefer another solution. For one, it wouldn't have all the same protections as the webstore, and I'd wonder if extensions would still find a way to access it - we have a reasonably centralized check in `PermissionsData::IsRestrictedUri()`, but I can't guarantee that's perfect. I'm also not really keen on protecting a part of [google.com](#) based on the path (rather than the domain). It'd theoretically mean that any [google.com](#) site could "opt out" of extensions by using `history.pushState()`, either intentionally or through some other script.

**Comment 12** by [thestig@chromium.org](#) on Wed, Jul 8, 2020, 1:38 PM EDT Project Member

Well, if extensions are free to navigate a tab to chrome:// URLs, then my idea probably won't work.

I didn't design `chrome.cloudPrintPrivate` and it took me a long time to find it's used in the registration flow on `chrome://devices`. AFAIK, the intended use case is for `chrome://devices` to navigate the user to [https://www.google.com/cloudprint/enable\\_chrome\\_connector/enable.html](https://www.google.com/cloudprint/enable_chrome_connector/enable.html), and that page use `chrome.cloudPrintPrivate` to magically get the local printer list and register them.

**Comment 13** by [rdevl...@chromium.org](#) on Wed, Jul 8, 2020, 1:48 PM EDT Project Member

Note: Filed [issue-4403303](#) to track disallowing (more) private APIs for hosted apps.

**Comment 14** by [rdevl...@chromium.org](#) on Fri, Jul 10, 2020, 6:38 PM EDT Project Member

Cc: [karandeepb@chromium.org](#)

**Comment 15** by [zachbutler@google.com](#) on Mon, Jul 13, 2020, 6:46 PM EDT Project Member

It seems the least risky option is to just have an exception for this Cloud Print URL? I know that's not ideal, but given Cloud Print's upcoming deprecation, would it be sufficient for the next ~6 months?

My concern with moving the API origin is that it could have unintended side effects we don't know about. But I'm also not familiar with what exactly that would entail, so perhaps I'm overestimating the risk.

**Comment 16** by [sheriffbot](#) on Thu, Jul 23, 2020, 1:38 PM EDT Project Member

thestig: Uh oh! This issue still open and hasn't been updated in the last 15 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 17** by [thestig@chromium.org](#) on Thu, Jul 30, 2020, 8:42 PM EDT Project Member

Security folks, is this something we can live with for ~6 more months until Cloud Print deprecation?

**Comment 18** by [creis@chromium.org](#) on Fri, Jul 31, 2020, 7:13 PM EDT Project Member

Cc: [adetaylor@chromium.org](#)

I'm not thrilled with leaving this unfixed until Cloud Print is gone, but maybe we can discuss the implications and make a call on that. Deprecations do have a habit of being delayed, and 6 months is already a long time to let this sit, so I'd prefer a fix if we can find a reasonable one in the meantime. Adding [adetaylor@](#) to get a second opinion.

In terms of implications and severity, this isn't the worst API to expose, but it is a bit of a privacy leak. IIUC, it leaks the names of the locally connected printers the user has, to an attacker who has control over their entire Google account already. Those local printers may overlap with the ones already accessible to the attacker via <https://www.google.com/cloudprint/#printers>, but only if the user has already gone through the flow from [comment 12](#). I don't think the bug allows an attacker to connect to those printers directly (e.g., no IP addresses are revealed), but leaking the names may reveal something about the user (e.g., where they work, network topology, private names). I'm curious if [adetaylor@](#) thinks that merits Medium or should be Low severity, and whether we need to prioritize a fix.

For fix options, I can understand that changing the origin used by CloudPrint isn't a good idea this late in the game.

I also see Devlin's point that URL based restrictions aren't ideal, since the victim URL can appear inside or outside the affected hosted app, and it's true that other Google URLs could pretend to be it to disable `executeScript`. Devlin, could content script logic instead disable `executeScript` inside the hosted app itself regardless of URL (e.g., based on a `SiteInstance` check)? That would limit the effect to cases where we legitimately loaded the URL of a Cloud Print hosted app in the normal way, and where the page wouldn't be able to be scripted by same-origin pages outside the hosted app anyway.

That restriction would admittedly affect other URLs loaded within the Cloud Print hosted app, such as the <https://clients5.google.com/pagead/drt/dn/> iframe on [https://www.google.com/cloudprint/enable\\_chrome\\_connector/enable.html](https://www.google.com/cloudprint/enable_chrome_connector/enable.html), but that might be ok for something hopefully going away within a year. The whole restriction could then go away at that time.

Thoughts?

**Comment 19** by [adetaylor@chromium.org](#) on Sat, Aug 1, 2020, 8:49 PM EDT Project Member

> IIUC, it leaks the names of the locally connected printers the user has, to an attacker who has control over their entire Google account already.

If that's an accurate description of the situation, I'd class this as Low, and I would be OK waiting for the inevitable 12 months until cloud print is `_actually_ deprecated` :) It seems to me that in most realistic cases, control of the Google account can yield lots of interesting information and exploitation possibilities. Getting the local printer names seems a minimal amount of extra information.

**Comment 20** by [creis@chromium.org](#) on Mon, Aug 3, 2020, 2:20 PM EDT Project Member

**Labels:** -Security\_Severity-Medium Security\_Severity-Low

[adetaylor@](#): Thanks. I'm dropping to Low severity accordingly. And thanks Devlin for preventing further instances of this type of bug with hosted apps in [issue-4403303](#)!

[thestig@](#): Is there an issue filed for deprecating / turning off Cloud Print that this can be marked blocked on?

Also, anyone should feel free to chime in if we've misunderstood the severity. It's obviously less than ideal to expose APIs like this to content scripts, but I'm glad we have a path to removing this last case.

**Comment 21** by [sheriffbot](#) on Mon, Aug 3, 2020, 2:59 PM EDT Project Member

**Labels:** -Pri-1 Pri-2

Setting Pri-2 to match security severity Low. 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 22** by [thestig@chromium.org](#) on Mon, Aug 3, 2020, 8:36 PM EDT Project Member  
**Blockedon:** 1112576

**Comment 23** by [thestig@chromium.org](#) on Mon, Aug 3, 2020, 8:37 PM EDT Project Member  
Note that this is not blocked on complete Cloud Print deprecation. It's just chrome://devices that needs to be removed.

**Comment 24** by [creis@chromium.org](#) on Tue, Aug 4, 2020, 6:54 PM EDT Project Member  
Thanks! Hopefully that's something that can be done early in the deprecation process.

**Comment 25** by [rdevl...@chromium.org](#) on Thu, Aug 6, 2020, 1:02 PM EDT Project Member  
I'm good with waiting for Cloud Print deprecation, and, as Charlie and Ade mentioned, I think if an attacker has access to [google.com](#), the printers aren't high on the list of concerns in practice.

> Devlin, could content script logic instead disable executeScript inside the hosted app itself regardless of URL (e.g., based on a SiteInstance check)?

Technically, yes, and I agree this would be a better check. The downside is that it'd be a fair amount of work to update all the necessary call sites to use the hosted app URL, and I'd wonder if there'd be anything else that breaks along the way. If we're okay waiting for deprecation, that's my preference.

**Comment 26** by [sheriffbot](#) on Wed, Aug 26, 2020, 1:38 PM EDT Project Member  
**Labels:** -M-84 Target-85 M-85

**Comment 27** by [sheriffbot](#) on Wed, Oct 7, 2020, 1:37 PM EDT Project Member  
**Labels:** -M-85 M-86 Target-86

**Comment 28** by [sheriffbot](#) on Fri, Oct 30, 2020, 6:46 PM EDT Project Member  
**Labels:** reward-potential

**Comment 29** by [sheriffbot](#) on Wed, Nov 18, 2020, 12:22 PM EST Project Member  
**Labels:** -M-86 M-87 Target-87

**Comment 30** by [creis@chromium.org](#) on Thu, Dec 3, 2020, 7:26 PM EST Project Member  
**Cc:** [rbpottter@chromium.org](#)  
I see [rbpottter@](#) has removed chrome://devices in [issue 1112576](#). Thanks! [thestig@](#), does that resolve the issue here?

**Comment 31** by [creis@chromium.org](#) on Mon, Dec 7, 2020, 8:24 PM EST Project Member  
**Owner:** [rbpottter@chromium.org](#)  
**Cc:** [thestig@chromium.org](#)  
**Components:** Services>CloudPrint

Looks like [thestig@](#) is on leave. [rbpottter@](#): I noticed that the cloudPrintPrivate API still seems to be around (e.g., chrome/browser/extensions/api/cloud\_print\_private/cloud\_print\_private\_api.h). [Comment 12](#) implies that chrome://devices was the only use of that API, and this bug is about a security issue due to that API. Now that chrome://devices is gone, would it be possible to remove that API as well to close this security bug? Thanks!

**Comment 32** by [rbpottter@chromium.org](#) on Thu, Dec 10, 2020, 9:59 PM EST Project Member  
Happy to go ahead and start a CL to remove it, if we're confident that was the only usage (I can try to find/dig around the [google.com/cloudprint](#) code if needed but I'm not really familiar with it or with this API). As noted in [comment 30](#), chrome://devices was removed in M88.

**Comment 33** by [bugdroid](#) on Thu, Jan 7, 2021, 2:09 PM EST Project Member  
The following revision refers to this bug:  
<https://chromium.googlesource.com/chromium/src/+c5f9e0438b670cc1c5077a39518ca056d46c642a>

commit [c5f9e0438b670cc1c5077a39518ca056d46c642a](#)  
Author: [rbpottter <rbpottter@chromium.org>](#)  
Date: Thu Jan 07 19:09:05 2021

Remove cloudPrintPrivate extension API

The only valid use case involved the chrome://devices page, which has been removed.

[Bug-1109749, 4462464](#)

Change-Id: [Ie1d62eecd00cec5e35fb76e7398c0ab40ea95b5f](#)  
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2585562>  
Reviewed-by: Achuth Bhandarkar <[achuth@chromium.org](#)>  
Reviewed-by: Devlin <[rdevlin.cronin@chromium.org](#)>  
Commit-Queue: Rebekah Potter <[rbpottter@chromium.org](#)>  
Cr-Commit-Position: refs/heads/master@{#841133}

[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud\\_print\\_app/DIR\\_METADATA](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud_print_app/DIR_METADATA)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/\\_api\\_features.json](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/_api_features.json)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/extensions/component\\_loader.cc](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/extensions/component_loader.cc)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/browser\\_resources.grd](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/browser_resources.grd)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/common/extensions/api/cloud\\_print\\_private.json](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/common/extensions/api/cloud_print_private.json)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/permissions/permission\\_set\\_unittest.cc](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/permissions/permission_set_unittest.cc)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud\\_print\\_app/OWNERS](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud_print_app/OWNERS)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud\\_print\\_private/cloud\\_print\\_private\\_apitest.cc](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud_print_private/cloud_print_private_apitest.cc)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/test/ext\\_auto/auto\\_provider/manifest.json](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/test/ext_auto/auto_provider/manifest.json)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/permissions/chrome\\_api\\_permissions.cc](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/permissions/chrome_api_permissions.cc)  
[modify] <https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/extensions/BUILD.gn>  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/api\\_sources.gni](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/api_sources.gni)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/extensions/browser/extension\\_function\\_histogram\\_value.h](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/extensions/browser/extension_function_histogram_value.h)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud\\_print\\_app/manifest.json](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/resources/cloud_print_app/manifest.json)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/\\_permission\\_features.json](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/common/extensions/api/_permission_features.json)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud\\_print\\_private/cloud\\_print\\_private\\_api.cc](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud_print_private/cloud_print_private_api.cc)  
[modify] <https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/test/BUILD.gn>  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/extensions/component\\_extensions\\_allowlist/allowlist.cc](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/chrome/browser/extensions/component_extensions_allowlist/allowlist.cc)  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud\\_print\\_private/cloud\\_print\\_private\\_api.h](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/browser/extensions/api/cloud_print_private/cloud_print_private_api.h)  
[modify] <https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/tools/metrics/histograms/enums.xml>  
[delete] [https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api\\_test/cloud\\_print\\_private/enable\\_chrome\\_connector/cloud\\_print\\_success\\_tests.js](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api_test/cloud_print_private/enable_chrome_connector/cloud_print_success_tests.js)

[delete]  
[https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api\\_test/cloud\\_print\\_private/enable\\_chrome\\_connector/cloud\\_print\\_success\\_tests.html](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api_test/cloud_print_private/enable_chrome_connector/cloud_print_success_tests.html)  
[delete]  
[https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api\\_test/cloud\\_print\\_private/enable\\_chrome\\_connector/cloud\\_print\\_incognito\\_failure\\_tests.js](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api_test/cloud_print_private/enable_chrome_connector/cloud_print_incognito_failure_tests.js)  
[modify] [https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/extensions/common/permissions/api\\_permission.h](https://crrev.com/c5f9e0438b670cc1c5077a39518ca056d46c642a/extensions/common/permissions/api_permission.h)  
[delete]  
[https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api\\_test/cloud\\_print\\_private/enable\\_chrome\\_connector/cloud\\_print\\_incognito\\_failure\\_tests.html](https://crrev.com/b7441ba363991c9f5b7087bed3bed845021f52a1/chrome/test/data/extensions/api_test/cloud_print_private/enable_chrome_connector/cloud_print_incognito_failure_tests.html)

**Comment 34** by [creis@chromium.org](mailto:creis@chromium.org) on Thu, Jan 7, 2021, 7:08 PM EST Project Member

**Status:** Fixed (was: Assigned)

Thanks rbpotter@! I think that should resolve this enough to be considered fixed.

Devlin, is there any followup we can do from your [comment 3](#)?

> This is obviously an exception. On the upside, a quick search seems to indicate that this is the `_only_` exception - I don't see any other restricted APIs that are available to hosted apps (other than the webstore).

I'm wondering if there's a way to prevent restricted APIs from being granted to hosted apps at this point, with the CWS as the lone exception.

**Comment 35** by [sheriffbot](#) on Fri, Jan 8, 2021, 12:43 PM EST Project Member

**Labels:** reward-topanel

**Comment 36** by [sheriffbot](#) on Fri, Jan 8, 2021, 1:59 PM EST Project Member

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

**Comment 37** by [rdevl...@chromium.org](#) on Fri, Jan 8, 2021, 5:38 PM EST Project Member

@34: Check out [issue-1403303](#) :) (mentioned this briefly in [#c13](#), but definitely easy to get lost in this shuffle)

Thank you for checking!

**Comment 38** by [creis@chromium.org](mailto:creis@chromium.org) on Fri, Jan 8, 2021, 6:08 PM EST Project Member

Fantastic! I thought I'd seen something like that. I've sent <https://chromium-review.googlesource.com/c/chromium/src/+2617873> to remove the CloudPrint extension ID from that allowlist, in case that's safe to do now.

**Comment 39** by [bugdroid](#) on Fri, Jan 8, 2021, 7:20 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+19bd4f137aca5b68dc8e144e2a98a8c964e98a48>

commit 19bd4f137aca5b68dc8e144e2a98a8c964e98a48

Author: Charlie Reis <[creis@chromium.org](mailto:creis@chromium.org)>

Date: Sat Jan 09 00:19:17 2021

Remove CloudPrint hosted app exception now that CloudPrint is gone.

We don't need to allow the CloudPrint hosted app to use restricted APIs after [r841133](#).

[Bug-1403303, 4400748](#)

Change-Id: If8965b276a53cd00fa6822f870b7db78d77dfef4

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2617873>

Commit-Queue: Charlie Reis <[creis@chromium.org](mailto:creis@chromium.org)>

Commit-Queue: Devlin <[rdevlin.cronin@chromium.org](mailto:rdevlin.cronin@chromium.org)>

Reviewed-by: Devlin <[rdevlin.cronin@chromium.org](mailto:rdevlin.cronin@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#841728}

[modify] [https://crrev.com/19bd4f137aca5b68dc8e144e2a98a8c964e98a48/tools/json\\_schema\\_compiler/feature\\_compiler.py](https://crrev.com/19bd4f137aca5b68dc8e144e2a98a8c964e98a48/tools/json_schema_compiler/feature_compiler.py)

**Comment 40** by [sheriffbot](#) on Thu, Jan 14, 2021, 4:22 PM EST Project Member

**Labels:** external\_security\_report

**Comment 41** by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Jan 20, 2021, 7:01 PM EST Project Member

**Labels:** -reward-potential

**Comment 42** by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, Feb 26, 2021, 1:08 PM EST Project Member

**Labels:** Release-0-M89

**Comment 43** by [adetaylor@google.com](mailto:adetaylor@google.com) on Mon, Mar 1, 2021, 7:29 PM EST Project Member

**Labels:** CVE-2021-21185 CVE\_description-missing

**Comment 44** by [amyressler@google.com](mailto:amyressler@google.com) on Tue, Mar 9, 2021, 12:59 PM EST Project Member

**Labels:** -CVE\_description-missing CVE\_description-submitted

**Comment 45** by [sheriffbot](#) on Wed, Mar 10, 2021, 8:05 PM EST Project Member

**Labels:** reward-potential

**Comment 46** by [zhangtiff@google.com](mailto:zhangtiff@google.com) on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

**Labels:** -reward-potential external\_security\_bug

**Comment 47** by [amyressler@google.com](mailto:amyressler@google.com) on Wed, Mar 17, 2021, 8:06 PM EDT Project Member

**Labels:** -reward-topanel reward-unpaid reward-1000

\*\*\* 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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

**Comment 48** by [amyressler@google.com](mailto:amyressler@google.com) on Wed, Mar 17, 2021, 8:30 PM EDT Project Member

Congratulations, David! The VRP Panel has decided to award you \$1,000 for this report. Thank you for your excellent report of this issue.

[Comment 49](#) by [amyressler@google.com](mailto:amyressler@google.com) on Thu, Mar 18, 2021, 1:29 PM EDT Project Member  
**Labels:** -reward-unpaid reward-inprocess

[Comment 50](#) by [sheriffbot](#) on Thu, Jun 24, 2021, 1:54 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