☆ Starred by 6 users

Owner:	caseq@chromium.org
CC:	gov...@chromium.org adetaylor@chromium.org yangguo@chromium.org rdevl...@chromium.org pbomm...@chromium.org caseq@chromium.org solomonkinard@chromium.org tjudkins@chromium.org dsv@google.com
Status:	Fixed *(Closed)*
Components:	Platform>DevTools Platform>Extensions
Modified:	Aug 28, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-3000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-81
Target-81
Merge-Rejected-81
Release-0-M83
CVE-2020-6471

Issue 1059577: Security: Possible to escape sandbox via devtools_page

Reported by derce...@gmail.com on Sun, Mar 8, 2020, 12:48 AM EST

Code

VULNERABILITY DETAILS
Using devtools_page, an extension can customize the devtools. The page referred to by the extension will be loaded whenever the devtools is shown.

Using this ability, an extension can download and run an executable once the user opens the devtools on any page, without requiring any further interaction.

VERSION
Chrome Version: Tested on 80.0.3987.132 (stable) and 82.0.4078.0 (canary)
Operating System: Windows 10, version 1909

REPRODUCTION CASE
Note that the demonstration here is Windows-specific.

1. Install the attached extension. Note that the manifest.json file in the extension contains a reference to the extension ID. You'll need to update this once Chrome has set an ID, then reload the extension. This wouldn't be an issue for a published extension, since the ID would be fixed in that case.
2. Load a page (it doesn't matter exactly what), then open the devtools.
3. Wait 4 seconds.
4. A cmd.exe instance should be started.

CREDIT INFORMATION
Reporter credit: David Erceg

devtools.js
2.0 KB View Download

manifest.json
300 bytes View Download

Comment 1 by derce...@gmail.com on Sun, Mar 8, 2020, 12:52 AM EST

In the demonstration above, there's a few steps being taken:

1. The devtools_page value contains a javascript: URL. This URL runs within the context of the devtools itself. This means that as soon as the devtools is opened (on any page), the extension has access to the devtools context.

Note that it isn't necessary to use a javascript: URL; the issue can be reproduced in the same sort of way when devtools_page refers to a file within the extension. However, using a javascript: URL simplifies the demonstration.

2. The page being debugged is navigated to chrome://downloads.

3. At this point, the goal is download and run an arbitrary executable without any further interaction. This is made more complicated by the fact that unsafe downloads may be need explicit approval from the user, both when downloading and when opening.

To work around this, the extension uses methods available via the full devtools protocol. Specifically, Page.setDownloadBehavior is first called in the following way:

parent.SDK.targetManager.mainTarget().pageAgent().setDownloadBehavior("allow", "C:\\Users\\Public");

This then means that when the target file is downloaded, it won't be marked as dangerous.

4. The extension then dispatches a key event to the chrome://downloads page via SDK.targetManager.mainTarget().inputAgent().dispatchKeyEvent. This event goes through the devtools protocol and is treated as a real event.

This means that when the extension calls openFileRequiringGesture in the context of the chrome://downloads page a short while later, the request succeeds as the page looks like it's had a recent user gesture.

The end result is that the executable that's downloaded is run without any other interaction from the user.

Comment 2 by mpdenton@google.com on Tue, Mar 10, 2020, 9:22 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: rdevl...@chromium.org
Cc: yangguo@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1

+rdevlin.cronin@ and yangguo@. Not sure if this is devtools or extensions issue. Perhaps extensions shouldn't be able to inject themselves into devtools for chrome:// protocol or other privileged protocols?

This may be a duplicate of ~~https://crbug.com/795595~~, but the user gesture bypass for the chrome downloads page is interesting.

Comment 3 by sheriffbot on Wed, Mar 11, 2020, 1:08 PM EDT Project Member

Labels: Target-81 M-81

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 tsepez@chromium.org on Wed, Mar 11, 2020, 1:12 PM EDT Project Member

Components: Platform>Extensions Platform>DevTools

Comment 5 by derce...@gmail.com on Thu, Mar 12, 2020, 3:26 PM EDT

For what it's worth, it's also possible to perform the same steps as above without any user interaction after extension install, provided the "debugger" permission is also set. There's an extension I've attached here that demonstrates this. Reproduction instructions are similar to those in the original demonstration:

1. Install the attached extension. Update the extension ID referenced in manifest.json then reload the extension.
2. Wait 6 seconds.
3. A cmd.exe instance should be started.

From what I can tell, the extension permissions prompt when specifying debugger and devtools_page is the same as when only specifying debugger, so the user might expect that the extension is only using the debugger permission.

background.js
863 bytes View Download

devtools.js
2.3 KB View Download

manifest.json
409 bytes View Download

page.html
123 bytes View Download

page.js
89 bytes View Download

service_worker.js
1 bytes View Download

Comment 6 by yangguo@chromium.org on Fri, Mar 13, 2020, 8:30 AM EDT Project Member

Similarly to related issues, I think that extensions should not have the ability to open devtools or have access to devtools UI.

Comment 7 by rdevl...@chromium.org on Wed, Mar 18, 2020, 7:42 PM EDT Project Member

Owner: caseq@chromium.org
Cc: rdevl...@chromium.org

Thanks for the report!

This is definitely a bug. Extensions shouldn't be allowed to attach and debug chrome:-scheme pages. We have a good bit of code around this, which is predominantly by overriding DevToolsAgentHostClient::MayAttachToURL() here [1]. That prevents attaching to restricted pages (which chrome:-scheme pages are) and also webui pages. So the fact that the extension is still able to send commands to it implies that that method isn't being correctly called or checked.

caseq@, mind taking a look from the devtools perspective, since it seems like this should be working if that method is being correctly called? Feel free to punt back to me if that's not the case.

[1] https://cs.chromium.org/chromium/src/chrome/browser/extensions/api/debugger/debugger_api.cc?l=372-381&rcl=0a1c4d9781d7327bb1dccd2ce3d9ad2a530a0103

Comment 8 by sheriffbot on Sun, Mar 22, 2020, 12:26 PM EDT Project Member

caseq: 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 9 by sheriffbot on Mon, Mar 23, 2020, 12:26 PM EDT Project Member

caseq: 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 10 by sheriffbot on Tue, Mar 24, 2020, 12:27 PM EDT Project Member

caseq: 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 11 by caseq@chromium.org on Tue, Mar 24, 2020, 7:24 PM EDT Project Member

Status: Started (was: Assigned)

Comment 12 by bugdroid on Wed, Mar 25, 2020, 5:10 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/1df0bf470f22368104de9aee7ec95d96c5b0232a

commit 1df0bf470f22368104de9aee7ec95d96c5b0232a
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Wed Mar 25 21:10:21 2020

DevTools extensions: validate devtools_page URLs

This ensures that the devtools_page URL has correct scheme and host,
both when loading the manifest and when pushing data to DevTools front-end.

~~Bug: 1059577~~
Change-Id: I69a7ccdccfae31781ead371a85d23df36f108665
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2118894
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#753369}

[modify] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/browser/devtools/devtools_ui_bindings.cc
[modify] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/common/extensions/chrome_manifest_url_handlers.cc
[modify] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/common/extensions/docs/templates/articles/devtools.html
[modify] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/common/extensions/manifest_tests/extension_manifests_devtools_unittest.cc
[add] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/test/data/extensions/manifest_tests/devtools_extension_invalid_page_url.json
[add] https://crrev.com/1df0bf470f22368104de9aee7ec95d96c5b0232a/chrome/test/data/extensions/manifest_tests/devtools_extension_page_url_https.json

Comment 13 by derce...@gmail.com on Thu, Mar 26, 2020, 12:00 AM EDT

I've attached a demonstration extension that shows how to download and run an executable, even if devtools_page is set to a page within the extension.

Reproduction instructions:

1. Install the attached extension.
2. Load a page, then open the devtools.
3. Wait 8 seconds.
4. A cmd.exe instance should be started.

This version of the extension relies on the fact that the devtools_page entry remains loaded in the devtools, no matter what the target page is and that it's possible to inspect a devtools window that the user has opened via chrome://inspect/.

These abilities mean that once the user has opened the devtools on a page (it doesn't matter what page), the extension can redirect to chrome://inspect/, then inspect the devtools window that was opened. At that stage, the extension has the ability to run code within the context of the devtools and the demonstration proceeds in the same way as above.

As an overview of the various situations:

1. devtools_page set to extension page, user opens devtools, possible to run executable.
2. devtools_page set to javascript: URL, no user interaction, possible to read local files and run code within the context of other extensions.
3. devtools_page set to javascript: URL, debugger permission also requested, no user interaction, possible to run executable.

devtools.html
127 bytes View Download

devtools.js
4.9 KB View Download

manifest.json
137 bytes View Download

Comment 14 by caseq@chromium.org on Fri, Mar 27, 2020, 3:23 PM EDT Project Member

Cc: caseq@chromium.org

~~Issue 1059676~~ has been merged into this issue.

Comment 15 by bugdroid on Mon, Mar 30, 2020, 2:24 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/4d33ef9730cae7a86b46690f434ced6cf8173642

commit 4d33ef9730cae7a86b46690f434ced6cf8173642
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Mon Mar 30 06:23:18 2020

DevTools: only allow inspectWorker if client can attach to browser

~~Bug: 1059577~~, 1064852
Change-Id: I2994be49f53aa8fc52fbd7cee543fa65521670f0
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2121434
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
Cr-Commit-Position: refs/heads/master@{#754408}

[modify] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/chrome/test/data/extensions/api_test/debugger_inspect_worker/background.js
[add] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/chrome/test/data/extensions/api_test/debugger_inspect_worker/inspected_page.html
[add] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/chrome/test/data/extensions/api_test/debugger_inspect_worker/manifest.json
[add] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/chrome/test/data/extensions/api_test/debugger_inspect_worker/service_worker.js

[modify] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/content/browser/devtools/protocol/service_worker_handler.cc
[modify] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/content/browser/devtools/protocol/service_worker_handler.h
[modify] https://crrev.com/4d33ef9730cae7a86b46690f434ced6cf8173642/content/browser/devtools/render_frame_devtools_agent_host.cc

Comment 16 by bugdroid on Wed, Apr 1, 2020, 6:27 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/devtools/devtools-frontend/+/a08cb9b5eb602e1bc0921629309ebdad5208f8d1

commit a08cb9b5eb602e1bc0921629309ebdad5208f8d1
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Wed Apr 01 22:27:20 2020

Disable extensions when inspecting DOM UI

This disables front-end extensions when DevTools are attached to
privileged pages.

~~Bug: 1059577~~, ~~795595~~
Change-Id: I0971fd993bee63eea347ffa800c3cc72e09ba334
Reviewed-on: https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+/2128732
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Benedikt Meurer <bmeurer@chromium.org>
Reviewed-by: Tim van der Lippe <tvanderlippe@chromium.org>

[modify] https://crrev.com/a08cb9b5eb602e1bc0921629309ebdad5208f8d1/front_end/extensions/ExtensionServer.js
[modify] https://crrev.com/a08cb9b5eb602e1bc0921629309ebdad5208f8d1/front_end/Tests.js

Comment 17 by bugdroid on Thu, Apr 2, 2020, 2:55 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/67fd81d2f51379aa9e89be61863b6f213524225c

commit 67fd81d2f51379aa9e89be61863b6f213524225c
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Thu Apr 02 06:54:10 2020

Roll src/third_party/devtools-frontend/src 0a34c98ea0b0..4d123409dc1a (2 commits)

https://chromium.googlesource.com/devtools/devtools-frontend.git/+log/0a34c98ea0b0..4d123409dc1a

git log 0a34c98ea0b0..4d123409dc1a --date=short --first-parent --format='%ad %ae %s'
2020-04-01 caseq@chromium.org Improve code hygiene in ExtensionServer
2020-04-01 caseq@chromium.org Disable extensions when inspecting DOM UI

Created with:
gclient setdep -r src/third_party/devtools-frontend/src@4d123409dc1a

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/devtools-frontend-chromium
Please CC devtools-waterfall-sheriff-onduty@grotations.appspotmail.com on the revert to ensure that a human
is aware of the problem.

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+/master/autoroll/README.md

~~Bug: chromium:1059577~~,~~chromium:1064519~~,~~chromium:795595~~
Tbr: devtools-waterfall-sheriff-onduty@grotations.appspotmail.com
Change-Id: I9b945356218e8de1b56c79f9b114606beab046d5
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2133415
Reviewed-by: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Commit-Queue: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/heads/master@{#755721}

[modify] https://crrev.com/67fd81d2f51379aa9e89be61863b6f213524225c/DEPS

Comment 18 by bugdroid on Fri, Apr 3, 2020, 3:48 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/3c0f2556708b39f7cb223ea33306a7fbb10ca01f

commit 3c0f2556708b39f7cb223ea33306a7fbb10ca01f
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Fri Apr 03 19:47:18 2020

DevTools: add tests for extensions on DOM UI pages

This is the chrome-side counterpart of
https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+/2128732

~~Bug: 1059577~~, ~~795595~~
Change-Id: Iec2ee772a42b4c7bc2249627c0839f7506f0cd1d
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2129344
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Commit-Position: refs/heads/master@{#756375}

[modify] https://crrev.com/3c0f2556708b39f7cb223ea33306a7fbb10ca01f/chrome/browser/devtools/devtools_sanity_browsertest.cc
[add] https://crrev.com/3c0f2556708b39f7cb223ea33306a7fbb10ca01f/chrome/test/data/devtools/extensions/chrome_scheme/devtools.html
[add] https://crrev.com/3c0f2556708b39f7cb223ea33306a7fbb10ca01f/chrome/test/data/devtools/extensions/chrome_scheme/devtools.js
[add] https://crrev.com/3c0f2556708b39f7cb223ea33306a7fbb10ca01f/chrome/test/data/devtools/extensions/chrome_scheme/manifest.json

Comment 19 by caseq@chromium.org on Fri, Apr 3, 2020, 4:02 PM EDT Project Member

Status: Fixed (was: Started)
Labels: Merge-Request-81

Requesting a merge to m81, but ultimately deferring it to the security team's judgement on whether the severity of the issue justifies merge at this stage.

Comment 20 by sheriffbot on Fri, Apr 3, 2020, 4:04 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: We are only 3 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

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

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

Comment 21 by pbommana@google.com on Fri, Apr 3, 2020, 6:06 PM EDT Project Member
Cc: adetaylor@chromium.org pbomm...@chromium.org gov...@chromium.org

Can this CL wait for next M81 respin?

So that the change will be well baked in lower channels before merging to M81 branch.

+adetaylor@(Security TPM), are you ok with it?

Comment 22 by gov...@chromium.org on Fri, Apr 3, 2020, 6:11 PM EDT Project Member

Also there are multiple changes listed in this bug. Will of them need a merge to M81 if we decide to take in for M81 respin?

Comment 23 by adetaylor@chromium.org on Fri, Apr 3, 2020, 6:12 PM EDT Project Member
Labels: -Merge-Review-81 Merge-Rejected-81

I think let's wait and have this roll into M83 organically. It doesn't look like the sort of complexity/security benefit ratio we'd want to merge into the current stable release. Thanks for asking though caseq@.

Comment 24 by sheriffbot on Sat, Apr 4, 2020, 1:55 PM EDT Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 25 by natashapabrai@google.com on Mon, Apr 6, 2020, 3:09 PM EDT Project Member
Labels: reward-topanel

Comment 26 by natashapabrai@google.com on Wed, Apr 8, 2020, 6:52 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 27 by natashapabrai@google.com on Wed, Apr 8, 2020, 6:55 PM EDT Project Member

Congrats! The Panel decided to award $3,000 for this report.

Comment 28 by natashapabrai@google.com on Wed, Apr 8, 2020, 7:04 PM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 29 by derce...@gmail.com on Fri, Apr 10, 2020, 7:07 PM EDT
About the fix in #c16:

One thing I've noticed is that the change doesn't have the desired result when a different scheme is used for DOM UI pages. For example, Edge uses edge:// rather than chrome://.

Comment 30 by caseq@chromium.org on Fri, Apr 10, 2020, 7:32 PM EDT Project Member

Thanks, that's a good point -- we should really pass the list of privileged schemes from the embedder (there's a TODO comment to that effect in the CL), or perhaps even just white-list http(s) there.

Comment 31 by bugdroid on Thu, May 7, 2020, 5:09 PM EDT Project Member
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/82b85893c49370f96ccb53573536dc1493daf8f3

commit 82b85893c49370f96ccb53573536dc1493daf8f3
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Thu May 07 21:07:58 2020

Revert "DevTools: add tests for extensions on DOM UI pages"

This reverts commit 3c0f2556708b39f7cb223ea33306a7fbb10ca01f.

Reason for revert: test is extremely flaky

Per https://analysis.chromium.org/p/chromium/flake-portal/flakes/occurrences?key=ag9zfmZpbmRpdC1mb3ItbWVyUgsSBUZsYWtlIkdjaHJvbWl1bUBicm93c2VyX3Rlc3RzQERldlRvb2xzRXh0ZW5zaW9uVGVzdC5UZXN0RXZhbHVhdGVPbkNocm9tZVNjaGVtZQw this flakily fails about 10 times an hour.

Original change's description:
> DevTools: add tests for extensions on DOM UI pages
>
> This is the chrome-side counterpart of
> https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+/2128732
>
> ~~Bug: 1059577~~, ~~705595~~
> Change-Id: Iec2ee772a42b4c7bc2249627c0839f7506f0cd1d
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2129344

> Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#756375}

TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,bmeurer@chromium.org

# Not skipping CQ checks because original CL landed > 1 day ago.

~~Bug: 1059577~~, ~~795595~~
Change-Id: I2919088167b064086b315d8c3a64df569d95c844
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2188512
Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/heads/master@{#766575}

[modify] https://crrev.com/82b85893c49370f96ccb53573536dc1493daf8f3/chrome/browser/devtools/devtools_sanity_browsertest.cc
[delete] https://crrev.com/3de250a49eedeb88c1e23fcc6429eba348f96161/chrome/test/data/devtools/extensions/chrome_scheme/devtools.html
[delete] https://crrev.com/3de250a49eedeb88c1e23fcc6429eba348f96161/chrome/test/data/devtools/extensions/chrome_scheme/devtools.js
[delete] https://crrev.com/3de250a49eedeb88c1e23fcc6429eba348f96161/chrome/test/data/devtools/extensions/chrome_scheme/manifest.json

Comment 32 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 33 by adetaylor@chromium.org on Mon, May 18, 2020, 11:58 AM EDT Project Member

Labels: CVE-2020-6471 CVE_description-missing

Comment 34 by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 35 by sheriffbot on Sat, Jul 11, 2020, 2:58 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

Comment 36 by bugdroid on Fri, Aug 28, 2020, 11:26 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/0f93d79ad9a6002933a5eebe000df8eca702b55a

commit 0f93d79ad9a6002933a5eebe000df8eca702b55a
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Sat Aug 29 03:24:55 2020

Reland "DevTools: add tests for extensions on DOM UI pages"

This reverts commit 82b85893c49370f96ccb53573536dc1493daf8f3.

Reason for revert: let's give this test another change. it seems to reliable pass for me locally and I think the original failure was rather due to a front-end race fixed here:
https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+/2242769

Original change's description:
> Revert "DevTools: add tests for extensions on DOM UI pages"
>
> This reverts commit 3c0f2556708b39f7cb223ea33306a7fbb10ca01f.
>
> Reason for revert: test is extremely flaky
>
> Per https://analysis.chromium.org/p/chromium/flake-portal/flakes/occurrences?key=ag9zfmZpbmRpdC1mb3ItbWVyUgsSBUZsYWtlIkdjaHJvbWl1bUBicm93c2VyX3Rlc3RzQERldlRvb2xzRXh0ZW5zaW9uVGVzdC5UZXN0RXZhbHVhdGVPbkNocm9tZVNjaGVtZQw this flakily fails about 10 times an hour.
>
> Original change's description:
> > DevTools: add tests for extensions on DOM UI pages
> >
> > This is the chrome-side counterpart of
> > https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+/2128732
> >
> > ~~Bug: 1059577~~, ~~795595~~
> > Change-Id: Iec2ee772a42b4c7bc2249627c0839f7506f0cd1d
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2129344
> > Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> > Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> > Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#756375}
>
> TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,bmeurer@chromium.org
>
> # Not skipping CQ checks because original CL landed > 1 day ago.
>
> ~~Bug: 1059577~~, ~~795595~~
> Change-Id: I2919088167b064086b315d8c3a64df569d95c844
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2188512
> Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>
> Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#766575}

TBR=dgozman@chromium.org,mek@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,bmeurer@chromium.org

# Not skipping CQ checks because original CL landed > 1 day ago.

~~Bug: 1059577~~
~~Bug: 795595~~
Change-Id: Ibd719500160685664de90415d718b88b4621b52e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2382487
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Commit-Position: refs/heads/master@{#802868}

[modify] https://crrev.com/0f93d79ad9a6002933a5eebe000df8eca702b55a/chrome/browser/devtools/devtools_sanity_browsertest.cc

[add] https://crrev.com/0f93d79ad9a6002933a5eebe000df8eca702b55a/chrome/test/data/devtools/extensions/chrome_scheme/devtools.html
[add] https://crrev.com/0f93d79ad9a6002933a5eebe000df8eca702b55a/chrome/test/data/devtools/extensions/chrome_scheme/devtools.js
[add] https://crrev.com/0f93d79ad9a6002933a5eebe000df8eca702b55a/chrome/test/data/devtools/extensions/chrome_scheme/manifest.json