☆ Starred by 4 users

| | |
|---|---|
| **Owner:** | caseq@chromium.org |
| **CC:** | bmeu...@chromium.org<br>rob@robwu.nl<br>yangguo@chromium.org<br>rdevl...@chromium.org<br>kozy@chromium.org<br>johannes@chromium.org<br>jonor...@microsoft.com<br>caseq@chromium.org<br>pfeldman@chromium.org<br>alph@chromium.org<br>mea...@chromium.org<br>solomonkinard@chromium.org<br>tjudkins@chromium.org<br>dsv@google.com |
| **Status:** | Fixed *(Closed)* |
| **Components:** | Platform>Extensions>API<br>Platform>DevTools>Platform |
| **Modified:** | Aug 28, 2020 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Windows, Chrome, Mac |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
reward-2000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
Target-68
Target-69
Target-70
CVE_description-submitted
Target-71
Target-72
Target-73
Target-74

### Issue 795595: Security: chrome.devtools.inspectedWindow.eval executes within privileged pages

Reported by green...@hotmail.com on Sun, Dec 17, 2017, 11:31 AM EST

Code

**VULNERABILITY DETAILS**
Extensions are normally not allowed to execute javascript within privileged pages for many reasons. Though it seems like we can use "chrome.devtools.inspectedWindow.eval" to execute JS in any page we want.

Given that the manifest contains permission for only "<all_urls>" it should not work within privileged pages. I think it should follow similar restrictions as "chrome.tabs.executeScript"

**VERSION**
Chrome Version: 63.0.3239.108 (Official Build) (64-bit)
Operating System: Windows 10 x64

**REPRODUCTION CASE**
**Please include a demonstration of the security bug, such as an attached HTML or binary file that reproduces the bug when loaded in Chrome. PLEASE make the file as small as possible and remove any content not required to demonstrate the bug.**

1. Install attached extension
2. Go to a privileged page like about:downloads
3. Open web inspector
4. Navigate to 'My panel'

**devtools-panels.zip**
5.2 KB Download

Comment 1 by elawrence@chromium.org on Mon, Dec 18, 2017, 11:42 AM EST Project Member

**Cc:** rdevl...@chromium.org
**Labels:** OS-Chrome OS-Linux OS-Mac OS-Windows
**Components:** Platform>Extensions>API Platform>DevTools>Platform

Interesting. Thanks for the report!

Comment 2 by elawrence@chromium.org on Mon, Dec 18, 2017, 11:43 AM EST Project Member

**Cc:** pfeldman@chromium.org
**Labels:** Security_Impact-Stable

Comment 3 by gov...@chromium.org on Sat, Dec 23, 2017, 10:24 AM EST Project Member

**Cc:** alph@chromium.org

Comment 4 by green...@hotmail.com on Sun, Dec 24, 2017, 8:13 AM EST

FWIW, we can also execute JS using the following:

```
    chrome.devtools.panels.elements.createSidebarPane("Font Properties",
        function(sidebar) {
          sidebar.setExpression('alert("Alert from setExpression")','test')
        });
```

Same behavior as inspectedWindow.eval

Comment 5 by alph@chromium.org on Mon, Dec 25, 2017, 10:03 PM EST Project Member

**Status:** Assigned (was: Unconfirmed)
**Owner:** kozy@chromium.org
**Cc:** dgozman@chromium.org

Comment 6 by green...@hotmail.com on Wed, Dec 27, 2017, 12:50 AM EST

Here is a more minimized testcase using both ways to execute JS. I removed the permissions setting within the manifest and it still works, seems like devtools extensions ignore it completely.

**PoC.zip**
1.7 KB Download

Comment 7 by rsesek@chromium.org on Wed, Dec 27, 2017, 7:55 PM EST Project Member

**Labels:** M-64 Security_Severity-Medium

Tentatively labeling as medium, since this does require the user to install an extension.

Comment 8 by green...@hotmail.com on Thu, Dec 28, 2017, 6:11 AM EST

It's also possible to automatically execute the JS as soon as the web console appears using the following (within devtools.js) instead:

```
chrome.devtools.panels.create(
  "My Panel",
  "icons/star.png",
  "devtools/panel/panel.html",
  function(panel){
          chrome.devtools.inspectedWindow.eval('alert()');
  }
);
```

Comment 9 by sheriffbot@chromium.org on Thu, Dec 28, 2017, 9:03 AM EST Project Member

**Labels:** Pri-1

Comment 10 by dgozman@chromium.org on Thu, Dec 28, 2017, 9:16 AM EST Project Member

I think this is a feature rather than a bug. It requires an extension with devtools permission to be installed, and DevTools being manually open by the user on chrome:// page.
What do security folks think?

Comment 11 by green...@hotmail.com on Thu, Dec 28, 2017, 12:20 PM EST

You could just ask a user to hold CTRL+SHFT+I and this would work, I don't think thats unlikely though definitely a slight mitigation. Past similar bugs have been considered security sensitive with medium severity: 456841, 38920, 30937, 42356, 83010
I also wonder if there is a problem with having devtool extensions abide by the manifest permission setting? I can't imagine that would break anything.

Comment 12 by sheriffbot@chromium.org on Mon, Jan 1, 2018, 9:00 AM EST Project Member

kozy: 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 13 by metzman@chromium.org on Tue, Jan 2, 2018, 7:15 PM EST Project Member

**Cc:** rob@robwu.nl

Comment 14 by kozy@chromium.org on Wed, Jan 3, 2018, 12:36 PM EST Project Member

**Owner:** caseq@chromium.org

Comment 15 by sheriffbot@chromium.org on Mon, Jan 15, 2018, 9:00 AM EST Project Member

caseq: Uh oh! This issue still open and hasn't been updated in the last 28 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 16 by mea...@chromium.org on Fri, Jan 26, 2018, 2:06 PM EST Project Member

caseq: Ping. Are you the right person for this bug?

Comment 17 by mea...@chromium.org on Fri, Jan 26, 2018, 2:06 PM EST Project Member

**Cc:** kozy@chromium.org

~~Issue 798184~~ has been merged into this issue.

Comment 18 by mea...@chromium.org on Fri, Jan 26, 2018, 2:08 PM EST Project Member

rob@robwu.nl's notes from ~~bug 798184~~:

"
Other affected APIs are:
https://developer.chrome.com/extensions/devtools_panels#method-ExtensionSidebarPane-setExpression
https://developer.chrome.com/extensions/devtools_inspectedWindow#method-reload

dgozman added a comment (https://bugs.chromium.org/p/chromium/issues/detail?id=795595#c10 ) where he questioned whether this is a feature/bug and cited some manual interaction requirements to support that claim. All of these interactions can be automated via extensions, as I have shown in the PoC in comment 2.

Extensions should not be able to automatically run scripts in privileged pages, since it can be used to completely compromise Chrome (and also run local programs, see ~~bug 798222~~).
"

There is additional information and a PoC in that bug as well.

Comment 19 by och...@chromium.org on Sun, Feb 18, 2018, 8:37 PM EST Project Member

Friendly ping from the security sheriff. dgozman, would do you think about rob's comment in #18?

Comment 20 by sheriffbot@chromium.org on Wed, Mar 7, 2018, 9:00 AM EST Project Member

**Labels:** -M-64 M-65

Comment 21 by sheriffbot@chromium.org on Wed, Apr 18, 2018, 9:01 AM EDT Project Member

**Labels:** -M-65 M-66

Comment 22 by green...@hotmail.com on Wed, May 16, 2018, 2:00 AM EDT

May I get an update on this issue? A similar problem ha been fixed in Firefox and I am planning to do a writeup somewhere around June.

Comment 23 by sheriffbot@chromium.org on Wed, May 30, 2018, 9:01 AM EDT Project Member

**Labels:** -M-66 M-67

Comment 24 by sheriffbot@chromium.org on Wed, Jul 25, 2018, 9:01 AM EDT Project Member

**Labels:** -M-67 Target-68 M-68

Comment 25 by sheriffbot@chromium.org on Wed, Sep 5, 2018, 9:02 AM EDT Project Member

**Labels:** -M-68 M-69 Target-69

Comment 26 by green...@hotmail.com on Thu, Sep 13, 2018, 4:30 AM EDT

Benign ping, any update on this?

Comment 27 by sheriffbot@chromium.org on Wed, Oct 17, 2018, 9:02 AM EDT Project Member

**Labels:** -M-69 Target-70 M-70

Comment 28 by kenrb@chromium.org on Mon, Nov 12, 2018, 12:06 PM EST Project Member

**Cc:** mea...@chromium.org

Just to note that the reporter has made this bug public: https://leucosite.com/WebExtension-Security-Part-2/

caseq@: Do you have any plans to work on this soon? This is a P1 that has been open for almost 11 months.

Comment 29 by sheriffbot@chromium.org on Wed, Dec 5, 2018, 9:03 AM EST Project Member

**Labels:** -M-70 Target-71 M-71

Comment 30 by sheriffbot@chromium.org on Wed, Jan 30, 2019, 9:03 AM EST Project Member

**Labels:** -M-71 Target-72 M-72

Comment 31 by sheriffbot@chromium.org on Wed, Mar 13, 2019, 9:03 AM EDT Project Member

**Labels:** -M-72 Target-73 M-73

Comment 32 by mea...@chromium.org on Fri, Apr 12, 2019, 7:27 PM EDT Project Member

caseq and other devtools folks, ping?

Comment 33 by sheriffbot@chromium.org on Wed, Apr 24, 2019, 9:04 AM EDT Project Member

**Labels:** -M-73 Target-74 M-74

Comment 34 by dgozman@chromium.org on Wed, May 8, 2019, 7:22 PM EDT Project Member

**Cc:** -dgozman@chromium.org

Comment 35 by sheriffbot@chromium.org on Thu, Jun 6, 2019, 9:07 AM EDT Project Member

**Labels:** -M-74 M-75 Target-75

Comment 36 by sheriffbot@chromium.org on Wed, Jul 31, 2019, 9:04 AM EDT Project Member

**Labels:** -M-75 M-76 Target-76

Comment 37 by sheriffbot@chromium.org on Wed, Sep 11, 2019, 9:06 AM EDT Project Member

**Labels:** -M-76 M-77 Target-77

Comment 38 by sheriffbot@chromium.org on Wed, Oct 23, 2019, 9:16 AM EDT Project Member

**Labels:** -M-77 Target-78 M-78

Comment 39 by caseq@chromium.org on Wed, Oct 30, 2019, 3:46 PM EDT Project Member

**Cc:** jonor...@microsoft.com caseq@chromium.org johannes@chromium.org

~~Issue 1019524~~ has been merged into this issue.

Comment 40 by caseq@chromium.org on Wed, Oct 30, 2019, 3:48 PM EDT Project Member

**Cc:** yangguo@chromium.org bmeu...@chromium.org

Comment 41 by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:17 AM EST Project Member

**Labels:** -M-78 Target-79 M-79

Comment 42 by sheriffbot@chromium.org on Wed, Feb 5, 2020, 10:52 AM EST Project Member

**Labels:** -M-79 M-80 Target-80

Comment 43 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: 1050577~~, ~~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 44 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:1050577~~,~~chromium:1064510~~,~~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 45 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: 1050577~~, ~~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 46 by sheriffbot on Thu, Apr 9, 2020, 12:33 PM EDT Project Member

**Labels:** -M-80 Target-81 M-81

Comment 47 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~~, ~~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}

[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 48 by adetaylor@google.com on Wed, May 13, 2020, 12:36 PM EDT Project Member

caseq@ do you consider this now fixed? If so please mark the bug Fixed so it can get picked up for release notes, etc.

Comment 49 by caseq@chromium.org on Fri, May 15, 2020, 3:53 PM EDT Project Member

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

I think we can close this, although there's a bit of the follow-up work (e.g. plumb proper set of restricted schemes, fix the test flakiness)

Comment 50 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

**Labels:** Release-0-M83

Comment 51 by sheriffbot on Sat, May 16, 2020, 3:01 PM EDT Project Member

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

Comment 52 by adetaylor@chromium.org on Mon, May 18, 2020, 11:59 AM EDT Project Member

**Labels:** CVE-2020-6482 CVE_description-missing

Comment 53 by natashapabrai@google.com on Tue, May 19, 2020, 10:27 AM EDT Project Member

**Labels:** reward-topanel

Comment 54 by sheriffbot on Tue, May 19, 2020, 3:25 PM EDT Project Member

**Labels:** Merge-Request-83

Requesting merge to beta M83 because latest trunk commit (756375) appears to be after beta branch point (756066).

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

Comment 55 by sheriffbot on Tue, May 19, 2020, 3:31 PM EDT Project Member

**Labels:** -Merge-Request-83 Merge-Review-83 Hotlist-Merge-Review

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 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), cindyb@(ChromeOS), srinivassista@(Desktop)

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

Comment 56 by cindyb@google.com on Tue, May 19, 2020, 5:45 PM EDT Project Member

**Labels:** -Merge-Review-83 Merge-Approved-83

Merge approved.

Comment 57 by natashapabrai@google.com on Wed, May 20, 2020, 9:31 PM EDT Project Member

**Labels:** -reward-topanel reward-unpaid reward-2000

*** 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 58 by natashapabrai@google.com on Wed, May 20, 2020, 9:48 PM EDT Project Member

Congrats! The Panel decided to award $2,000 for this report

Comment 59 by adetaylor@chromium.org on Wed, May 20, 2020, 11:44 PM EDT Project Member

**Labels:** -CVE_description-missing CVE_description-submitted

Comment 60 by srinivassista@google.com on Thu, May 28, 2020, 1:02 PM EDT Project Member

Please complete the merge to M83 branch asap, as we will cut the re-spin RC tomorrow.

Comment 61 by caseq@chromium.org on Thu, May 28, 2020, 3:46 PM EDT Project Member

**Labels:** -Merge-Approved-83

No merge required -- the original fix made it into trunk as of 83.0.4103.0: https://storage.googleapis.com/chromium-find-releases-static/67f.html#67fd81d2f51379aa9e89be61863b6f213524225c

The subsequent CL is only a test, no need to merge that.

Comment 62 by natashapabrai@google.com on Fri, May 29, 2020, 5:45 PM EDT Project Member

**Labels:** -reward-unpaid reward-inprocess

Comment 63 by sheriffbot on Sat, Aug 22, 2020, 3:04 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 64 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
```