Starred by 3 users

Owner:	caseq@chromium.org
CC:	adetaylor@chromium.org yangguo@chromium.org rdevl...@chromium.org pbomm...@chromium.org caseq@chromium.org pfeldman@chromium.org dgozman@chromium.org sigurds@chromium.org petermarshall@chromium.org solomonkinard@chromium.org tjudkins@chromium.org dsv@google.com
Status:	Fixed *(Closed)*
Components:	Platform>Extensions>API Platform>DevTools
Modified:	Dec 8, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
Target-84
Target-85
M-85
merge-merged-4183
merge-merged-85
merge-merged-4240
merge-merged-86
Release-2-M85

Issue 1113558: Security: Possible to navigate frames not attached to the debugger using the chrome.debugger API

Reported by derce...@gmail.com on Thu, Aug 6, 2020, 2:39 AM EDT

Code

VULNERABILITY DETAILS

When using the chrome.debugger API, one of the methods an extension can call is Page.navigate. That method can navigate both the root frame and child frames. However, because the method is missing checks to see whether the debugger is attached to the specified frame, an extension can attach to a parent frame, then navigate any child frames, regardless of whether or not they're attached.

This allows the extension to escape the sandbox if the current browser isn't the system default browser, or if the user opens the devtools (perhaps because the extension has advertised devtools_page functionality). It otherwise allows an extension to script pages it normally wouldn't have access to: devtools: pages, file: pages, chrome-extension: pages and a few different chrome: pages.

VERSION

Chrome Version: Tested on 84.0.4147.105 (stable) and 86.0.4224.0 (canary)
Operating System: Windows 10, version 1909

REPRODUCTION CASE

1. Install the attached extension.
2. Once installed, the extension will open page.html in a new tab.
3. Once page.html has loaded, the extension will attach to it using chrome.debugger.attach and use Page.navigate to navigate an iframe on the page to devtools://devtools/bundled/inspector.html. This navigation will result in the debugger being detached from the page (since the extension doesn't have access to devtools: pages).
4. The extension will then reattach the debugger to the page (at this point, only the top frame will be attached and not the iframe).
5. Using Page.navigate, the extension will navigate the iframe to a javascript URL:

```
chrome.debugger.sendCommand({tabId: tab.id}, "Page.navigate", {url: "javascript:console.log('Code run from: ' + location.href)", frameId: childFrameId});
```

This will work even though the debugger isn't attached to the iframe and the extension can't interact with it otherwise.

CREDIT INFORMATION

Reporter credit: David Erceg

background.js
2.1 KB View Download

manifest.json
213 bytes View Download

page.html
103 bytes View Download

Comment 1 by derce...@gmail.com on Thu, Aug 6, 2020, 2:50 AM EDT

As mentioned in the summary, it's possible for the extension to escape the sandbox if the current browser isn't the default browser. That's because the extension can use the fact that it can script a devtools: page to run code within the Feedback app and then open a local file (using the behavior described in ~~issue 1106456~~).

It's also possible for the extension to escape the sandbox if the user opens the devtools. This is because once the extension can script a devtools: page, it can add a

console pin. That console pin will then allow for a downloaded executable to be opened using the steps described in ~~issue 1067382~~.

An extension can script a file: page by going through the same steps as above with a file: URL instead of a devtools: URL.

Finally, an extension can script chrome-extension: pages and a few different chrome: pages:

- chrome://blob-internals
- chrome://devices
- chrome://print
- chrome://serviceworker-internals

Scripting those pages is a bit more complicated than scripting a devtools: or file: page, since chrome-extension: and chrome: pages disallow execution of javascript: URLs:

https://source.chromium.org/chromium/chromium/src/+/master:extensions/renderer/dispatcher.cc;l=259;drc=ecb5c38ef1ddf1f3cc70577d60a0df42e63f15f7

https://source.chromium.org/chromium/chromium/src/+/master:content/renderer/render_thread_impl.cc;l=1019;drc=f7ff8bd538149a24f1ad6799fc626c17276d889a

However, since the extension can script a devtools: page, it can call:

InspectorFrontendHost.setInjectedScriptForOrigin

from within the context of a devtools: page. It can then navigate to one of the above pages in an iframe using Page.navigate (at which point the injected script will run). The will work for the chrome: pages above because none of them have any preventions on being loaded within a frame. That is, most chrome: pages specify the following headers:

Content-Security-Policy: ... frame-ancestors 'none';
X-Frame-Options: DENY

While the pages listed above specify neither of those headers. That means it's possible to navigate to them in an iframe on an arbitrary page using Page.navigate.

I can provide demonstrations of each of the above, if necessary.

Comment 2 by derce...@gmail.com on Thu, Aug 6, 2020, 2:55 AM EDT

I believe the cause of this behavior is fairly simple:

There are a number of devtools protocol methods that accept a frameId parameter (e.g. Page.createIsolatedWorld, Page.setDocumentContent, Page.getResourceContent, etc). When those methods are called, they perform the frame lookup against the set of inspected frames:

https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/inspector/identifiers_factory.cc;l=71;drc=2a373a2d09cf559f4812db03c94b51b193981ca8

If a frame isn't attached to the debugger, it won't be in that set.

However, when calling Page.navigate, the method that performs the frame lookup iterates through all subframes:

https://source.chromium.org/chromium/chromium/src/+/master:content/browser/devtools/protocol/handler_helpers.cc;l=18;drc=56989e01067d8ae440a9868a009800b3950a0570

Which then means Page.navigate can navigate any subframe, regardless of whether it's attached to the debugger.

Comment 3 by xinghuilu@chromium.org on Thu, Aug 6, 2020, 4:39 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: sigurds@chromium.org
Cc: rdevl...@chromium.org yangguo@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows
Components: Platform>Extensions>API Platform>DevTools

Thanks for the detailed report! The security threat is that a malicious extension is able to go beyond the current browser profile and escape sandbox, when the current browser isn't the default browser. The affected devtools api is Page.navigate.

sigurds@, could you take a look at this issue and evaluate if #c2 is the root cause? Thanks!

Comment 4 by sigurds@chromium.org on Fri, Aug 7, 2020, 3:31 AM EDT Project Member

Cc: pfeldman@chromium.org caseq@chromium.org

Thanks for assigning this to me. I refactored the code (that means: moved it unchanged to a helper method to use it in other places as well) that looks for the frame in https://crrev.com/c/2332820, but the original was introduced here: https://chromium-review.googlesource.com/885422 (Jan 2018).

This also means that this is not a recently introduced vulnerability, but most probably present in all released versions since 2018.

Comment 5 by sigurds@chromium.org on Fri, Aug 7, 2020, 4:23 AM EDT Project Member

I don't think that the filtering of the frames is the problem. The use-case for Page.navigate is precisely to allow it to navigate any frame (from the CDP client perspective). That we expose this functionality to extensions is problematic.

Note that https://bugs.chromium.org/p/chromium/issues/detail?id=1113565 also uses Page.navigate (there with a file URL), circumventing permissions.

I think Page.navigate shouldn't be (fully) exposed to extensions.

caseq@: Do you agree with my analysis?

Comment 6 by sheriffbot on Fri, Aug 7, 2020, 2:00 PM EDT Project Member

Labels: Target-84 M-84

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 Fri, Aug 7, 2020, 2:40 PM EDT Project Member

Labels: 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 caseq@chromium.org on Fri, Aug 7, 2020, 8:44 PM EDT Project Member

Cc: dgozman@chromium.org

Comment 9 by sigurds@chromium.org on Mon, Aug 10, 2020, 4:58 AM EDT Project Member

Dmitry, I'm observing that even after Andrey's fix, the extension is allowed to navigate a frame to a devtools:// URL. (It doesn't seem to be able to use page navigate to execute a script in it, though).

Should we allow an extension to navigate a frame to a devtools:// URL?

Comment 10 by sigurds@chromium.org on Mon, Aug 10, 2020, 5:11 AM EDT Project Member

Cc: petermarshall@chromium.org

Peter, maybe you have some background here you can share as well?

Comment 11 by sigurds@chromium.org on Mon, Aug 10, 2020, 6:25 AM EDT Project Member

I think we should restrict Page.navigate in such a way that Page.navigate is only allowed if the client that initiates the Page.navigate can also attach (i.e. we should use MayAttachToURL to check that). Dmitry, does that sound reasonable to you? If so, could you advice on how to do this?

Comment 12 by dgozman@chromium.org on Mon, Aug 10, 2020, 10:19 AM EDT Project Member

This makes sense. I think we can just call DevToolsAgentHostClient::MayAttachToURL from PageHandler::Navigate to prevent this.

Comment 13 by sigurds@chromium.org on Mon, Aug 10, 2020, 10:41 AM EDT Project Member

I'm having trouble getting to the instance of DevToolsAgentHostClient from there, do you have an idea?

Comment 14 by dgozman@chromium.org on Mon, Aug 10, 2020, 5:28 PM EDT Project Member

re #c13: yeah, I don't see an easy way currently. We can pass the owner DevToolsSession in the constructor, either to PageHandler or all subclasses of DevToolsDomainHandler.

Comment 15 by bugdroid on Wed, Aug 19, 2020, 2:13 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/4838b76ae48797760fd8a362b4dc15325ccddcf5

commit 4838b76ae48797760fd8a362b4dc15325ccddcf5
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Wed Aug 19 06:10:05 2020

Add more checks for chrome.debugger extensions

~~Bug: 1113558~~, ~~1113565~~
Change-Id: I99f2e030f9a38f1ffd6b6adc760ba15e5d231f96
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2342277
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Sigurd Schneider <sigurds@chromium.org>
Reviewed-by: Yang Guo <yangguo@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
Cr-Commit-Position: refs/heads/master@{#799514}

[modify] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/4838b76ae48797760fd8a362b4dc15325ccddcf5/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 16 by bugdroid on Wed, Aug 19, 2020, 5:42 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/5a809a08fd5ca32cb8d594664416db2f2dc8ebdc

commit 5a809a08fd5ca32cb8d594664416db2f2dc8ebdc
Author: Christian Dullweber <dullweber@chromium.org>
Date: Wed Aug 19 09:41:22 2020

Revert "Add more checks for chrome.debugger extensions"

This reverts commit 4838b76ae48797760fd8a362b4dc15325ccddcf5.

Reason for revert: 1119297

Original change's description:
> Add more checks for chrome.debugger extensions
>
> ~~Bug: 1113558~~, ~~1113565~~
> Change-Id: I99f2e030f9a38f1ffd6b6adc760ba15e5d231f96
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2342277
> Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> Reviewed-by: Sigurd Schneider <sigurds@chromium.org>
> Reviewed-by: Yang Guo <yangguo@chromium.org>
> Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#799514}

TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org

Change-Id: I01ad12ca99ac75197f9073e2c6c9d0eaa0d95147
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
~~Bug: 1113558~~
~~Bug: 1113565~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2362920
Reviewed-by: Christian Dullweber <dullweber@chromium.org>
Commit-Queue: Christian Dullweber <dullweber@chromium.org>
Cr-Commit-Position: refs/heads/master@{#799558}

[modify] https://crrev.com/5a809a08fd5ca32cb8d594664416db2f2dc8ebdc/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[delete] https://crrev.com/dda5b70c005af869ec6f5850bd46d83e8008bff5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[delete] https://crrev.com/dda5b70c005af869ec6f5850bd46d83e8008bff5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[delete] https://crrev.com/dda5b70c005af869ec6f5850bd46d83e8008bff5/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/5a809a08fd5ca32cb8d594664416db2f2dc8ebdc/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/5a809a08fd5ca32cb8d594664416db2f2dc8ebdc/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/5a809a08fd5ca32cb8d594664416db2f2dc8ebdc/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 17 by bugdroid on Fri, Aug 21, 2020, 3:32 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/a064db74c8734fbf47de2f3a3503832514857173

commit a064db74c8734fbf47de2f3a3503832514857173

Author: Andrey Kosyakov <caseq@chromium.org>
Date: Fri Aug 21 19:31:34 2020

Reland "Add more checks for chrome.debugger extensions"

This reverts commit 5a809a08fd5ca32cb8d594664416db2f2dc8ebdc.

Reason for revert: I don't think the test failure is related. Please note it stopped before the revert landed (build no 91007 vs. 91010). This must have been a flake, or a independent failure that has been fixed by one of the front-end rolls.

Original change's description:
> Revert "Add more checks for chrome.debugger extensions"
>
> This reverts commit 4838b76ae48797760fd8a362b4dc15325ccddcf5.
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > ~~Bug: 1113558~~, ~~1113565~~
> > Change-Id: I99f2e030f9a38f1ffd6b6adc760ba15e5d231f96
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2342277
> > Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> > Reviewed-by: Sigurd Schneider <sigurds@chromium.org>
> > Reviewed-by: Yang Guo <yangguo@chromium.org>
> > Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> > Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#799514}
>
> TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org
>
> Change-Id: I01ad12ca99ac75197f9073e2c6c9d0eaa0d95147
> No-Presubmit: true
> No-Tree-Checks: true
> No-Try: true
> ~~Bug: 1113558~~
> ~~Bug: 1113565~~
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2362920
> Reviewed-by: Christian Dullweber <dullweber@chromium.org>
> Commit-Queue: Christian Dullweber <dullweber@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#799558}

TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org,dullweber@chromium.org

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

~~Bug: 1113558~~
~~Bug: 1113565~~
Change-Id: Ic98fc037028a210204b7935b0b8e50e4e36e2397
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2368446
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Commit-Position: refs/heads/master@{#800682}

[modify] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/a064db74c8734fbf47de2f3a3503832514857173/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 18 by sheriffbot on Mon, Aug 24, 2020, 1:37 PM EDT Project Member

sigurds: 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 19 by adetaylor@google.com on Mon, Aug 24, 2020, 1:42 PM EDT Project Member

caseq@ do you deem this fixed? If so please mark as such.

Comment 20 by sheriffbot on Wed, Aug 26, 2020, 1:37 PM EDT Project Member

Labels: -M-84 Target-85 M-85

Comment 21 by sigurds@chromium.org on Mon, Aug 31, 2020, 4:49 AM EDT Project Member

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

Since you already fixed (part of this) issue, I'm re-assigning to you caseq@.

Comment 22 by caseq@chromium.org on Mon, Aug 31, 2020, 9:13 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 23 by adetaylor@google.com on Tue, Sep 1, 2020, 11:36 AM EDT Project Member

Labels: Merge-Request-85

caseq@ Sheriffbot will soon ask whether this should be merged back to 85 so I'll shortcut the process. As a high severity bug we'd like to do so, but only if you consider it has virtually zero stability/compatibility consequences. Please comment. We're likely to be cutting a branch for an M85 security refresh tomorrow.

Comment 24 by sheriffbot on Tue, Sep 1, 2020, 11:38 AM EDT Project Member

Labels: -Merge-Request-85 Merge-Review-85 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), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 25 by sheriffbot on Tue, Sep 1, 2020, 3:09 PM EDT Project Member

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

Comment 26 by caseq@chromium.org on Tue, Sep 1, 2020, 3:40 PM EDT Project Member

This looks mostly safe to me, but let's follow our usual process and let it bake for some time on canary and beta. As discussed with Srinivas, let's target it for the next re-spin of m85.

> 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

Yes, as a high severity security issue.

> 2. Links to the CLs you are requesting to merge.

https://chromium.googlesource.com/chromium/src.git/+/a064db74c8734fbf47de2f3a3503832514857173, as referred in #16

> 3. Has the change landed and been verified on master/ToT?

Yes.

> 4. Why are these changes required in this milestone after branch?

Because of the timing of us learning of this issue and fixing it.

> 5. Is this a new feature?

No.

> 6. If it is a new feature, is it behind a flag using finch?

N/A

Comment 27 by srinivassista@google.com on Tue, Sep 1, 2020, 5:45 PM EDT Project Member

Labels: Merge-Request-86

Adding merge-request-86 so this can go into next beta and bake so it can be included in the second security re-spin

Comment 28 by sheriffbot on Tue, Sep 1, 2020, 5:49 PM EDT Project Member

Labels: -Merge-Request-86 Merge-Review-86

This bug requires manual review: Reverts referenced in bugdroid comments after merge request.
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: govind@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 29 by pbommana@google.com on Fri, Sep 4, 2020, 11:11 PM EDT Project Member

Please reply to comment#28, which helps in merge decision.

Comment 30 by pbommana@google.com on Sun, Sep 6, 2020, 2:50 PM EDT Project Member

Cc: adetaylor@chromium.org pbomm...@chromium.org
Labels: -Merge-Review-86 Merge-Approved-86

Approving the change for M86 Branch :4240, Please goahead and get the Change merged asap.

+Adetaylor9Secuirty TPM) fyi

Comment 31 by adetaylor@google.com on Mon, Sep 7, 2020, 10:38 PM EDT Project Member

Labels: reward-topanel

Comment 32 by bugdroid on Tue, Sep 8, 2020, 1:52 PM EDT Project Member

Labels: -merge-approved-86 merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/9940472e708a4003aee9edf9da42d68fde591e08

commit 9940472e708a4003aee9edf9da42d68fde591e08
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Tue Sep 08 17:50:37 2020

[m86] Reland "Add more checks for chrome.debugger extensions"

TBR=rdevlin.cronin@chromium.org

This reverts commit 5a809a08fd5ca32cb8d594664416db2f2dc8ebdc.

Reason for revert: I don't think the test failure is related. Please note it stopped before the revert landed (build no 91007 vs. 91010). This must have been a flake, or a independent failure that has been fixed by one of the front-end rolls.

Original change's description:
> Revert "Add more checks for chrome.debugger extensions"
>
> This reverts commit 4838b76ae48797760fd8a362b4dc15325ccddcf5.
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > ~~Bug: 1113559~~, ~~1113565~~
> > Change-Id: I99f2e030f9a38f1ffd6b6adc760ba15e5d231f96
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2342277
> > Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> > Reviewed-by: Sigurd Schneider <sigurds@chromium.org>
> > Reviewed-by: Yang Guo <yangguo@chromium.org>
> > Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> > Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#799514}
>
> TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org
>
> Change-Id: I01ad12ca99ac75197f9073e2c6c9d0eaa0d95147
> No-Presubmit: true
> No-Tree-Checks: true
> No-Try: true
> ~~Bug: 1113559~~
> ~~Bug: 1113565~~
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2362920
> Reviewed-by: Christian Dullweber <dullweber@chromium.org>
> Commit-Queue: Christian Dullweber <dullweber@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#799558}

TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org,dullweber@chromium.org

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

(cherry picked from commit a064db74c8734fbf47de2f3a3503832514857173)

~~Bug: 1113559~~
~~Bug: 1113565~~
Change-Id: Ic98fc037028a210204b7935b0b8e50e4e36e2397
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2368446
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#800682}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2398884
Cr-Commit-Position: refs/branch-heads/4240@{#506}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/9940472e708a4003aee9edf9da42d68fde591e08/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 33 by adetaylor@google.com on Wed, Sep 9, 2020, 7:25 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 34 by adetaylor@google.com on Wed, Sep 9, 2020, 7:26 PM EDT Project Member

Congratulations! The VRP panel has decided to award $5000 for this bug.

Comment 35 by adetaylor@google.com on Thu, Sep 10, 2020, 1:42 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 36 by srinivassista@google.com on Fri, Sep 11, 2020, 12:48 PM EDT Project Member

Is the issue looking good on Beta ? If so is it ready for Merge to M85 , we can wait for more beta coverage until middle of next week before merging to M85 for more data

Comment 37 by adetaylor@google.com on Tue, Sep 15, 2020, 1:05 PM EDT Project Member

Labels: -Merge-Review-85 Merge-Approved-85

Approving merge to M85, branch 4183. Please merge, assuming things are looking good in Canary and beta.

Comment 38 by srinivassista@google.com on Thu, Sep 17, 2020, 4:51 PM EDT Project Member

Please complete your merge before 12pm PST on friday 9/18/2020.

Comment 39 by bugdroid on Fri, Sep 18, 2020, 6:36 PM EDT Project Member

Labels: -merge-approved-85 merge-merged-85 merge-merged-4183

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503

commit 3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503
Author: Andrey Kosyakov <caseq@chromium.org>

Date: Fri Sep 18 22:35:09 2020

[m85] Reland "Add more checks for chrome.debugger extensions"

TBR=rdevlin.cronin@chromium.org

This reverts commit 5a809a08fd5ca32cb8d594664416db2f2dc8ebdc.

Reason for revert: I don't think the test failure is related. Please note it stopped before the revert landed (build no 91007 vs. 91010). This must have been a flake, or a independent failure that has been fixed by one of the front-end rolls.

Original change's description:
> Revert "Add more checks for chrome.debugger extensions"
>
> This reverts commit 4838b76ae48797760fd8a362b4dc15325ccddcf5.
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > ~~Bug: 1112558~~, ~~1112565~~
> > Change-Id: I99f2e030f9a38f1ffd6b6adc760ba15e5d231f96
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2342277
> > Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
> > Reviewed-by: Sigurd Schneider <sigurds@chromium.org>
> > Reviewed-by: Yang Guo <yangguo@chromium.org>
> > Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
> > Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
> > Cr-Commit-Position: refs/heads/master@{#799514}
>
> TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org
>
> Change-Id: I01ad12ca99ac75197f9073e2c6c9d0eaa0d95147
> No-Presubmit: true
> No-Tree-Checks: true
> No-Try: true
> ~~Bug: 1112558~~
> ~~Bug: 1112565~~
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2362920
> Reviewed-by: Christian Dullweber <dullweber@chromium.org>
> Commit-Queue: Christian Dullweber <dullweber@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#799558}

TBR=dgozman@chromium.org,rdevlin.cronin@chromium.org,caseq@chromium.org,yangguo@chromium.org,sigurds@chromium.org,dullweber@chromium.org

(cherry picked from commit a064db74c8734fbf47de2f3a3503832514857173)

(cherry picked from commit 9940472e708a4003aee9edf9da42d68fde591e08)

~~Bug: 1112558~~
~~Bug: 1112565~~
Change-Id: Ic98fc037028a210204b7935b0b8e50e4e36e2397
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2368446
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#800682}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2398884
Cr-Original-Commit-Position: refs/branch-heads/4240@{#506}
Cr-Original-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2419133
Cr-Commit-Position: refs/branch-heads/4183@{#1863}
Cr-Branched-From: 740e9e8a40505392ba5c8e022a8024b3d018ca65-refs/heads/master@{#782793}

[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcdea503/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 40 by adetaylor@google.com on Mon, Sep 21, 2020, 1:18 PM EDT Project Member

Labels: Release-2-M85

Comment 41 by sheriffbot on Tue, Dec 8, 2020, 1:52 PM EST 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