




☆ Starred by 3 users

Owner:

caseq@chromium.org

CC:

adetaylor@chromium.org
 yangguo@chromium.org
rdevl...@chromium.org
jun.k...@microsoft.com
yu...@chromium.org
caseq@chromium.org
adetaylor@google.com
lukasza@chromium.org
dgozman@chromium.org
 sigurds@chromium.org
 dsv@google.com

Status:

Fixed (Closed)

Components:

Platform>DevTools>Platform

Modified:

Dec 8, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Windows, Chrome, Mac

Pri:

1

Type:

Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
reward-15000
Target-84
Target-85
M-85
merge-merged-4183
merge-merged-85
merge-merged-4240
merge-merged-86
Release-2-M85

Issue 1114636: Security: Possible for extension to escape sandbox via Target.setAutoAttach and Target.sendMessageToTarget

Reported by derce...@gmail.com on Mon, Aug 10, 2020, 5:32 AM EDT

🔗 Code

VULNERABILITY DETAILS

When using the chrome.debugger API, one of the methods an extension can call is Target.setAutoAttach. That method will attach all cross-process subframes (of the currently debugged page) to the debugger.

Once that's been done, an extension can call Target.sendMessageToTarget to dispatch a protocol message to an attached frame. Because the frame will have been attached in a higher privileged access mode (kRegular vs kAutoAttachOnly), additional protocol methods will be available to it.

By forwarding the appropriate protocol messages through the frame, an extension can attach to chrome://downloads and open a downloaded executable, which allows the extension to escape the sandbox.

VERSION

Chrome Version: Tested on 84.0.4147.105 (stable) and 86.0.4229.0 (canary)
Operating System: Windows 10, version 1909

REPRODUCTION CASE

1. Install the attached extension.
2. After a couple of seconds, the target executable (in this case, Process Explorer) should be started.

CREDIT INFORMATION

Reporter credit: David Erceg

background.js
5.2 KB [View](#) [Download](#)

manifest.json
244 bytes [View](#) [Download](#)

page.html
304 bytes [View](#) [Download](#)

Comment 1 by derce...@gmail.com on Mon, Aug 10, 2020, 5:38 AM EDT

The demonstration extension here performs a few steps:

1. The extension downloads the target executable.
2. It then opens chrome://downloads in a new tab.
3. Once chrome://downloads has loaded, the extension opens page.html in a new tab.
4. Once page.html has loaded, the extension attaches to it using chrome.debugger.attach.
5. It then calls Target.setAutoAttach. This will result in the subframe on the page being attached to the debugger in kRegular mode.
6. It then requests that the subframe attach to the chrome://downloads page. This is done by sending a Target.attachToTarget message to the subframe via Target.sendMessageToTarget.
7. The extension then sends a key event to the downloads page, by relaying Input.dispatchKeyEvent through the suframe using Target.sendMessageToTarget. This input event is needed to ensure that the downloaded file can be opened (which is something that requires a recent user gesture).
8. The extension then calls Runtime.evaluate via Target.sendMessageToTarget. The expression passed to the Runtime.evaluate call will run within the context of the

chrome://downloads page and open the executable downloaded in step 1.

One thing worth noting is that I don't think these steps will work in the same way under Linux, since any file the extension downloads won't be marked as executable.

However, another devtools protocol method the extension can call through an auto attached subframe is `Browser.setDownloadBehavior`. That allows a custom downloads directory to be set.

So an extension on Linux could first determine the path to the user's home directory (by attaching to a file:///home/ page and examining the contents) then overwrite something like `/home/{user}/.profile`. That file may then be sourced and any embedded commands executed when the user next logs in graphically.

Overwriting an existing file will work, since when the "behavior" parameter passed to `Browser.setDownloadBehavior` is "allow", existing files will be overwritten when downloading.

[Comment 2](#) by [derce...@gmail.com](#) on Mon, Aug 10, 2020, 5:45 AM EDT

When an extension calls `chrome.debugger.attach`, `ExtensionDevToolsClientHost::MayAttachToBrowser` returns false and the `TargetHandler` is constructed in `kAutoAttachOnly` mode:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/render_frame_devtools_agent_host.cc;l=334;drc=f2cfa81dccb4ede16a8b637158a0e0c5b21672af

When calling `Target.setAutoAttach`, all cross-process subframes are attached:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/protocol/target_auto_attacher.cc;l=184;drc=74a68a32bb8cc4f5db3abe45d8243637db1aa40

When attaching the frames, the following `MayAttachToBrowser` call:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/render_frame_devtools_agent_host.cc;l=327;drc=f2cfa81dccb4ede16a8b637158a0e0c5b21672af

resolves to:

https://source.chromium.org/chromium/chromium/src/+master:content/public/browser/devtools_agent_host_client.cc;l=13;drc=0788b1d419f78050f114ffefd1f68cd88d1dab

Which always returns true.

That then means that when `TargetHandler` is constructed, the access mode is set to `kRegular`:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/render_frame_devtools_agent_host.cc;l=333;drc=f2cfa81dccb4ede16a8b637158a0e0c5b21672af

So a number of methods within the `Target` namespace that are blocked when the access mode is `kAutoAttachOnly` can then be called.

Note that although all cross-process subframes will be attached to the debugger, it's not possible to interact with them via `chrome.debugger.sendCommand`. This is because the agent hosts associated with the subframes won't be represented in the list of attached client hosts that are maintained for extensions:

https://source.chromium.org/chromium/chromium/src/+master:chrome/browser/extensions/api/debugger/debugger_api.cc;l=499;drc=6ac77aad9d92fc74fba600c817fae15c30c5697

On the other hand, when using `Target.sendMessageToTarget`, the lookup is performed against the set of attached sessions:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/protocol/target_handler.cc;l=709;drc=6cf20e7892749db10432df68cfe7a6d16f629c67

This set is updated via the following call when attaching via `Target.setAutoAttach` or `Target.attachToTarget`:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/devtools/protocol/target_handler.cc;l=360;drc=6cf20e7892749db10432df68cfe7a6d16f629c67

[Comment 3](#) by [xinghuilu@chromium.org](#) on Mon, Aug 10, 2020, 7:11 PM EDT

Status: Assigned (was: Unconfirmed)

Owner: [dgozman@chromium.org](#)

Cc: [dgozman@chromium.org](#) [sigurds@chromium.org](#) [yu...@chromium.org](#) [caseq@chromium.org](#)

Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows

Components: Platform>DevTools>Platform

Thanks for the detailed report! [dgozman@](#), could you take a look at this issue and evaluate if `#c2` is the root cause? Thanks!

[Comment 4](#) by [dgozman@chromium.org](#) on Mon, Aug 10, 2020, 8:36 PM EDT

Owner: [caseq@chromium.org](#)

[Comment 5](#) by [sigurds@chromium.org](#) on Tue, Aug 11, 2020, 3:30 AM EDT

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

[Comment 6](#) by [sigurds@chromium.org](#) on Tue, Aug 11, 2020, 4:12 AM EDT

Dmitry, could you explain the security design behind the attach modes `kRegular` and `kAutoAttachOnly`?

From the description above, it seems a lot is going wrong:

- Why does the attach in step (5) get mode `kRegular`?
- It seems strange that `sendMessageToTarget` can send a "`Target.attachToTarget`" message

What is the proper fix?

I think `Target.sendMessageToTarget` should only be allowed for targets the session can also attach to.

Additionally, I would forbid `Target.attachToTarget` via `sendMessageToTarget`, but I don't know the implications.

In general, looking at the three recent security bugs in this area we might be in for a redesign of our security here.

[Comment 7](#) by [sigurds@chromium.org](#) on Tue, Aug 11, 2020, 6:17 AM EDT

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

[Comment 8](#) by [sigurds@chromium.org](#) on Tue, Aug 11, 2020, 8:44 AM EDT

This particular repro also relies on non-flattened auto attach mode. Maybe we should go forward and deprecate non-flattened mode right now?

[Comment 9](#) by [dgozman@chromium.org](#) on Tue, Aug 11, 2020, 11:58 AM EDT

re `#c6`:

> Why does the attach in step (5) get mode `kRegular`?

This is a bug. At the time we introduced security checks, targets infrastructure was already in place, so this particular place was missed.

> It seems strange that sendMessageToTarget can send a "Target.attachToTarget" message
Well, if you are attached to the target, you should be able to send any messages to it, in particular to attach to its subtargets. I think this is overall fine, as long as we properly handle specific restrictions like MayAttachToBrowser.

> In general, looking at the three recent security bugs in this area we might be in for a redesign of our security here.
This area definitely needs some love :)

> Maybe we should go forward and deprecate non-flattened mode right now?
Sure, we can go ahead and deprecate it. There is an issue for that [1]. However, we cannot remove it any time soon, unfortunately, due to heavy usage in legacy clients.

[1] <https://bugs.chromium.org/p/chromium/issues/detail?id=991325>

Comment 10 by [sheriffbot](#) on Tue, Aug 11, 2020, 1:59 PM EDT

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 11 by [sheriffbot](#) on Tue, Aug 11, 2020, 2:39 PM EDT

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 12 by [yangguo@chromium.org](#) on Wed, Aug 12, 2020, 4:50 PM EDT

Dmitry, do you have more details on these legacy clients, and whether they have plans to migrate? If not, waiting them indefinitely does not sound like a good path forward.

Comment 13 by [dgozman@chromium.org](#) on Wed, Aug 12, 2020, 6:12 PM EDT

Well, Target domain is public, so we don't know what do the clients in the wild do with it.

I know that Telemetry, ChromeDriver, Puppeteer, Playwright, Visual Studio Code, Lighthouse - all use Target domain, but some of these might be already using the flatten version. Extensions with chrome.debugger permission can be using it as well, and we don't support flatten mode there, IIRC.

Github search [1] brings some usages in mozilla remote, nwjs, a Go client called web-exfiltration, and 100 more search result pages. I don't know whether they are actually using Target domain, in legacy or flatten mode.

[1] <https://github.com/search?q=Target.attachedToTarget&type=Code>

Comment 14 by [sigurds@chromium.org](#) on Mon, Aug 17, 2020, 3:23 AM EDT

I think Target.sendMessageToTarget should only be possible for targets the client can attach to.

Comment 15 by [sheriffbot](#) on Mon, Aug 24, 2020, 1:37 PM EDT

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 16 by [sheriffbot](#) on Wed, Aug 26, 2020, 1:37 PM EDT

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

Comment 17 by [bugdroid](#) on Fri, Aug 28, 2020, 2:56 PM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+814a27f8522b6cddcce1a8f6a3b8fb37128ecf9>

commit 814a27f8522b6cddcce1a8f6a3b8fb37128ecf9

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Fri Aug 28 18:55:17 2020

Delegate TargetHandler::Session permission checks to the root client

~~bug-1114536~~

Change-Id: Iba3865206d7e80b363ec69180ac05e20b56aade2

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2380855>

Reviewed-by: Dmitry Gozman <dgozman@chromium.org>

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Commit-Queue: Andrey Kosyakov <caseq@chromium.org>

Cr-Commit-Position: refs/heads/master@{#802736}

[modify] https://crrev.com/814a27f8522b6cddcce1a8f6a3b8fb37128ecf9/chrome/browser/extensions/api/debugger/debugger_apitest.cc

[add] https://crrev.com/814a27f8522b6cddcce1a8f6a3b8fb37128ecf9/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/background.js

[add] https://crrev.com/814a27f8522b6cddcce1a8f6a3b8fb37128ecf9/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/manifest.json

[add] https://crrev.com/814a27f8522b6cddcce1a8f6a3b8fb37128ecf9/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/page.html

[modify] https://crrev.com/814a27f8522b6cddcce1a8f6a3b8fb37128ecf9/content/browser/devtools/protocol/target_handler.cc

Comment 18 by [caseq@chromium.org](#) on Fri, Aug 28, 2020, 5:00 PM EDT

Status: Fixed (was: Assigned)

Fixed by the commit referenced above. Thanks for the report, David, a very impressive work as usually!

Some random comments on the discussion above:

- (re #66) "Target.sendMessageToTarget should only be allowed for targets the session can also attach to" -- that's already the case. Actually, we only send it to the targets we previously attached to; the bug is in that DevToolsAgentHostClient implemented by DevToolsTargetHandler::Session is a more permission than the original one;

- it would be nice to deprecate non-flat mode for extensions (and it is generally deprecated already), but it turns out we actually don't support flat mode for extensions right now -- so this should be fixed first ([crbug.com/1123159](https://bugs.chromium.org/p/chromium/issues/detail?id=1123159))

Comment 19 by [sheriffbot](#) on Sat, Aug 29, 2020, 3:08 PM EDT

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

Comment 20 by [sheriffbot](#) on Sat, Aug 29, 2020, 3:28 PM EDT

Labels: Merge-Request-85

Requesting merge to stable M85 because latest trunk commit (802736) appears to be after stable branch point (782793).

Requesting merge to beta M85 because latest trunk commit (802736) appears to be after beta branch point (782793).

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

[Comment 21](#) by [sheriffbot](#) on Sat, Aug 29, 2020, 3:32 PM EDT

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), bindusuvama@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

[Comment 22](#) by [adetaylor@google.com](#) on Mon, Aug 31, 2020, 10:50 AM EDT

Labels: reward-topanel

[Comment 23](#) by [adetaylor@google.com](#) on Mon, Aug 31, 2020, 1:46 PM EDT

Labels: Merge-Request-86

caseq@ please could you comment on any stability or compatibility risks from merging this back to stable? As a high severity security bug we'd normally merge this back to M86 and M85 so long as you think it's nearly zero risk. If there's any chance this could break compatibility, perhaps merging to M86 is a good compromise?

[Comment 24](#) by [adetaylor@google.com](#) on Mon, Aug 31, 2020, 1:46 PM EDT

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

[Comment 25](#) by [sheriffbot](#) on Tue, Sep 1, 2020, 1:49 PM EDT

Labels: -Merge-Request-86 Hotlist-Merge-Approved Merge-Approved-86

Your change meets the bar and is auto-approved for M86. Please go ahead and merge the CL to branch 4240 (refs/branch-heads/4240) manually. Please contact milestone owner if you have questions.

Merge instructions: <https://www.chromium.org/developers/how-tos/drover>

Owners: govind@(Android), bindusuvama@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

[Comment 26](#) by [caseq@chromium.org](#) on Tue, Sep 1, 2020, 3:43 PM EDT

I wouldn't be too concerned about breaking compatibility for the extensions that are doing "this" :-). Let's start with m86 anyway, and follow up with a merge to m85, in a while, provided it caused no regression and you think this is useful.

[Comment 27](#) by [adetaylor@chromium.org](#) on Tue, Sep 1, 2020, 3:44 PM EDT

SGTM.

[Comment 28](#) by [adetaylor@google.com](#) on Wed, Sep 2, 2020, 6:38 PM EDT

Labels: -reward-topanel reward-unpaid reward-15000

*** 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 29](#) by [adetaylor@google.com](#) on Wed, Sep 2, 2020, 6:40 PM EDT

Congratulations! The VRP panel has decided to award \$15,000 for this report.

[Comment 30](#) by [adetaylor@google.com](#) on Thu, Sep 3, 2020, 11:14 AM EDT

Labels: -reward-unpaid reward-inprocess

[Comment 31](#) by [pbommana@google.com](#) on Sat, Sep 5, 2020, 11:32 AM EDT

Please merge your change to M86 branch 4240 ASAP. Thank you.

[Comment 32](#) by [sheriffbot](#) on Mon, Sep 7, 2020, 12:07 PM EDT

Cc: [adetaylor@google.com](#)

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

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

Thanks for your time! To disable nags, add the Disable-Nags label.

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

[Comment 33](#) Deleted

[Comment 34](#) by [bugdroid](#) on Tue, Sep 8, 2020, 6:34 PM EDT

Labels: merge-merged-4240

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+845cf2d928ea18078eebe9b25be4b14776c7e5ec>

commit [845cf2d928ea18078eebe9b25be4b14776c7e5ec](#)

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Tue Sep 08 22:32:50 2020

Delegate TargetHandler::Session permission checks to the root client

(cherry picked from commit [814a27f8522b6cddcce1a8f6a3b8fb37128ecf9](#))

TBR: rdevlin.cronin@chromium.org

[Bug-4114636](#)

Change-Id: [Iba3865206d7e80b363ec69180ac05e20b56aae2](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2380855>

Reviewed-by: Dmitry Gozman <dgozman@chromium.org>

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Commit-Queue: Andrey Kosyakov <caseq@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#802736}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2387414>

Reviewed-by: Andrey Kosyakov <caseq@chromium.org>

Cr-Commit-Position: refs/branch-heads/4240@{#539}

Cr-Branched-From: [f297677702651916bbf65e59c0d4bbd4ce57d1ee](#)-refs/heads/master@{#800218}

[modify] https://crrev.com/845cf2d928ea18078eebe9b25be4b14776c7e5ec/chrome/browser/extensions/api/debugger/debugger_apitest.cc

[add] https://crrev.com/845cf2d928ea18078eebe9b25be4b14776c7e5ec/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/background.js

[add] https://crrev.com/845cf2d928ea18078eebe9b25be4b14776c7e5ec/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/manifest.json

[add] https://crrev.com/845cf2d928ea18078eebe9b25be4b14776c7e5ec/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/page.html

[modify] https://crrev.com/845cf2d928ea18078eebe9b25be4b14776c7e5ec/content/browser/devtools/protocol/target_handler.cc

[Comment 35](#) by srinivassista@google.com on Fri, Sep 11, 2020, 12:48 PM EDT

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 36](#) by adetaylor@google.com on Tue, Sep 15, 2020, 1:05 PM EDT

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 37](#) by bugdroid on Thu, Sep 17, 2020, 1:32 AM EDT

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+503e8d49042e964487d479adbcf00748a489915b>

commit [503e8d49042e964487d479adbcf00748a489915b](#)

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Thu Sep 17 05:28:26 2020

[m85] Delegate TargetHandler::Session permission checks to the root client

(cherry picked from commit [814a27f8522b6cddcce1a8f6a3b8fb37128ecf9](#))

(cherry picked from commit [845cf2d928ea18078eebe9b25be4b14776c7e5ec](#))

TBR: rdevlin.cronin@chromium.org

[Bug-4114636](#)

Change-Id: [Iba3865206d7e80b363ec69180ac05e20b56aae2](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2380855>

Reviewed-by: Dmitry Gozman <dgozman@chromium.org>

Reviewed-by: Devlin <rdevlin.cronin@chromium.org>

Commit-Queue: Andrey Kosyakov <caseq@chromium.org>

Cr-Original-Original-Commit-Position: refs/heads/master@{#802736}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2387414>

Reviewed-by: Andrey Kosyakov <caseq@chromium.org>

Cr-Original-Commit-Position: refs/branch-heads/4240@{#539}

Cr-Original-Branched-From: [f297677702651916bbf65e59c0d4bbd4ce57d1ee](#)-refs/heads/master@{#800218}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2413347>

Cr-Commit-Position: refs/branch-heads/4183@{#1847}

Cr-Branched-From: [740e9e8a40505392ba5c8e022a8024b3d018ca65](#)-refs/heads/master@{#782793}

[modify] https://crrev.com/503e8d49042e964487d479adbcf00748a489915b/chrome/browser/extensions/api/debugger/debugger_apitest.cc

[add] https://crrev.com/503e8d49042e964487d479adbcf00748a489915b/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/background.js

[add] https://crrev.com/503e8d49042e964487d479adbcf00748a489915b/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/manifest.json

[add] https://crrev.com/503e8d49042e964487d479adbcf00748a489915b/chrome/test/data/extensions/api_test/debugger_auto_attach_permissions/page.html

[modify] https://crrev.com/503e8d49042e964487d479adbcf00748a489915b/content/browser/devtools/protocol/target_handler.cc

[Comment 38](#) by adetaylor@google.com on Mon, Sep 21, 2020, 1:18 PM EDT

Labels: Release-2-M85

[Comment 39](#) by sheriffbot on Sat, Dec 5, 2020, 1:51 PM EST

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 40](#) by jun.k...@microsoft.com on Tue, Dec 8, 2020, 3:16 AM EST

Cc: lukasza@chromium.org

lukasza@, isn't it possible to distrust 'Input.dispatchKeyEvent' from WebUI renderer and check actual user click in the browser process?

[Comment 41](#) by jun.k...@microsoft.com on Tue, Dec 8, 2020, 3:18 AM EST

Cc: jun.k...@microsoft.com