




☆ Starred by 3 users

Owner:

caseq@chromium.org

CC:

 yangguo@chromium.org
rdevl...@chromium.org
dgozman@chromium.org
 sigurds@chromium.org
 dsv@google.com

Status:

Fixed (Closed)

Components:

Platform>DevTools

Modified:

Dec 28, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Windows, Chrome, Mac

Pri:

1

Type:

Bug-Security

reward-5000

Security_Impact-Stable

Security_Severity-Medium

allpublic

reward-inprocess

Target-85

M-85

merge-merged-4183

merge-merged-85

merge-merged-4240

merge-merged-86

Release-2-M85

Issue 1113565: Security: Extensions can use chrome.debugger API to access contents of local files

Reported by derce...@gmail.com on Thu, Aug 6, 2020, 3:06 AM EDT

🔗 Code

VULNERABILITY DETAILS

Typically, extensions can't access local files without explicit user permission. However, by using the chrome.debugger API, an extension can navigate an iframe on a page to a file: location, then capture the contents of that page using the Page.captureSnapshot devtools protocol method.

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. Ensure that "Allow access to file URLs" isn't checked.
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 file:///c:/:. This navigation will result in the debugger being detached from the page (since the extension doesn't have access to local files).
4. The extension will then reattach the debugger to the page.
5. It will then call Page.captureSnapshot and log the result to the console:

```
chrome.debugger.sendCommand([tabId: tab.id], "Page.captureSnapshot", {}, function (result) {  
  console.log(result.data);  
});
```

This output should contain the contents of the file: iframe and can be seen by opening the devtools for the extension's background page.

CREDIT INFORMATION

Reporter credit: David Erceg

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

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

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

Comment 1 by xinghuilu@chromium.org on Thu, Aug 6, 2020, 4:48 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: caseq@chromium.org

Cc: yangguo@chromium.org rdevl...@chromium.org

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

Components: Platform>DevTools

Thanks for the report. I wonder if the underlying issue is similar to <https://crbug.com/1050976>.

caseq@, handed over to you to decide on whether it is a duplicate. Thanks!

Comment 2 by hablich@chromium.org on Fri, Aug 7, 2020, 3:39 AM EDT Project Member

Cc: sigurds@chromium.org

Comment 3 by sigurds@chromium.org on Fri, Aug 7, 2020, 4:30 AM EDT Project Member

IUC, this means that an extension (regardless of permissions) can get the contents of everything the browser can navigate to.

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

Also note related bug [crbug.com/4443558](#), in which Page.navigate is used to execute JavaScript.

Comment 5 by [sheriffbot](#) on Fri, Aug 7, 2020, 2:15 PM EDT Project Member

Labels: Target-85 M-85

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 6 by [sheriffbot](#) on Fri, Aug 7, 2020, 2:51 PM EDT Project Member

Labels: Pri-1

Setting Pri-1 to match security severity Medium. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

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

Cc: dgozman@chromium.org

Comment 8 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: 4443558, 4443555~~

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 9 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: 4443558, 4443555~~

> 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-Pre-submit: true

No-Tree-Checks: true

No-Try: true

~~Bug: 4443558~~

~~Bug: 4443555~~

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 10 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/+a064db74c8734fb47de2f3a3503832514857173>

commit [a064db74c8734fb47de2f3a3503832514857173](#)
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 [4838b76ae48797760fd8a362b4dc15325coddcf5](#).
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > [Bug-1112558](#), [1112555](#)
> > Change-Id: I99f2e030f9a38f1ffdb6adc760ba15e5d231f96
> > 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-1112555](#)
> 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-1112558](#)

[Bug-1112555](#)

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/a064db74c8734fb47de2f3a3503832514857173/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/a064db74c8734fb47de2f3a3503832514857173/content/browser/devtools/render_frame_devtools_agent_host.h

Comment 11 by [sheriffbot](#) on Sat, Aug 22, 2020, 1:36 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 12 by adetaylor@google.com on Mon, Aug 24, 2020, 1:41 PM EDT Project Member

caseq@ is this commit intended to fix this bug? If so please mark it as fixed.

Comment 13 by [sheriffbot](#) on Sun, Sep 6, 2020, 1:37 PM EDT Project Member

caseq: Uh oh! This issue still open and hasn't been updated in the last 29 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 14 by [bugdroid](#) on Tue, Sep 8, 2020, 1:52 PM EDT Project Member

Labels: 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 4838b76ae48797760fd8a362b4dc15325cdddcf5.
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > [Bug-1112568](#), [1112565](#)
> > Change-Id: I99f2e030f9a38f1ff6b6adc760ba15e5d231f96
> > 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-1112568](#)
> [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

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

(cherry picked from commit a064db74c8734bf47de2f3a3503832514857173)

[Bug-1112568](#)

[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-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 15 by [bugdroid](#) on Fri, Sep 18, 2020, 6:36 PM EDT Project Member

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

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+3b5f65c0aeca53ee01eb8caf3b93f3bbf0dea503>

commit 3b5f65c0aeca53ee01eb8caf3b93f3bbf0dea503

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 4838b76ae48797760fd8a362b4dc15325cdddcf5.
>
> Reason for revert: 1119297
>
> Original change's description:
> > Add more checks for chrome.debugger extensions
> >
> > [Bug-1112568](#), [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-1113558
> Bug-1113556
> 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 a064db74c8734fb47de2f3a3503832514857173)

(cherry picked from commit 9940472e708a4003aee9edf9da42d68fde591e08)

Bug-1113558

Bug-1113556

```
Change-Id: Icf98fc037028a210204b7935b0b8e50e4e36e2397
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/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/chrome/browser/extensions/api/debugger/debugger_apitest.cc
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/background.js
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/inspected_page.html
[add] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/chrome/test/data/extensions/api_test/debugger_navigate_subframe/manifest.json
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/content/browser/devtools/devtools_instrumentation.cc
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/content/browser/devtools/render_frame_devtools_agent_host.cc
[modify] https://crrev.com/3b5f65c0aeca53ee01eb8caf3b93f3bbfcd503/content/browser/devtools/render_frame_devtools_agent_host.h
```

Comment 16 by caseq@chromium.org on Mon, Sep 21, 2020, 1:31 PM EDT Project Member
Status: Fixed (was: Assigned)

Comment 17 by adetaylor@google.com on Mon, Sep 21, 2020, 1:32 PM EDT Project Member
Labels: Release-2-M85

Comment 18 by sheriffbot on Mon, Sep 21, 2020, 3:10 PM EDT Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 19 by adetaylor@google.com on Mon, Sep 28, 2020, 12:00 AM EDT Project Member
Labels: reward-topanel

Comment 20 by adetaylor@google.com on Wed, Sep 30, 2020, 6:49 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 21 by adetaylor@google.com on Wed, Sep 30, 2020, 6:59 PM EDT Project Member
Congratulations! The VRP panel has decided to award \$5000 for this bug.

Comment 22 by adetaylor@google.com on Thu, Oct 1, 2020, 2:33 PM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 23 by sheriffbot on Mon, Dec 28, 2020, 1:50 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