

☆ Starred by 3 users


Owner:

caseq@chromium.org

CC:


tommycli@chromium.org

bmeu...@chromium.org

 yangguo@chromium.org

rdevl...@chromium.org


dpa...@chromium.org

 sigurds@chromium.org

mea...@chromium.org

solomonkinard@chromium.org

tjudkins@chromium.org

 dsv@google.com

Status:

Fixed (Closed)

Components:

Platform>DevTools

Platform>Extensions

Modified:

Oct 30, 2021

Backlog-Rank:

----

Editors:

----

EstimatedDays:

----

NextAction:

----

OS:

Linux, Windows, Chrome, Mac, Fuchsia

Pri:

1

Type:

Bug-Security

Merge-na

reward-5000

Security\_Impact-Stable

Deadline-Exceeded

Security\_Severity-High

allpublic

reward-inprocess

CVE\_description-submitted

Target-88

Target-84

Target-83

Target-85

Target-86

Target-87

Target-89


Target-90

FoundIn-83

M-91

**Issue 1101897: Security: Possible to escape sandbox via devtools\_page (alternative method)**

Reported by [derce...@gmail.com](#) on Fri, Jul 3, 2020, 12:40 AM EDT

 Code

**VULNERABILITY DETAILS**

In [issue 105677](#), a method was provided for escaping the sandbox via devtools\_page. That issue relied on the fact that embedded extensions would remain active once the devtools was opened, no matter the target page.

That issue was fixed by updating the devtools to disable extensions when navigating to a privileged page. As noted in one of the CLs for that fix, there's still a potential timing issue present. Here, a method is presented that should allow an extension to reliably run code within the target page, even after it's been navigated to a privileged location. That then allows the extension to escape the sandbox.

**VERSION**

Chrome Version: Tested on 83.0.4103.116 (stable) and 86.0.4190.4 (canary)  
Operating System: Windows 10, version 1909

**REPRODUCTION CASE**

1. Install the attached extension.
2. Open the devtools on a non-privileged page.
3. The extension will go through a series of steps (described further below) to run code within the context of a privileged page (devtools://devtools/bundled/inspector.html).
4. Wait about 25 seconds.
5. The target executable (in this case, Process Explorer) should be started.

**CREDIT INFORMATION**

Reporter credit: David Erceg

**background.js**  
540 bytes [View](#) [Download](#)

**chrome\_inspect.js**  
1.1 KB [View](#) [Download](#)

**devtools.js**  
3.1 KB [View](#) [Download](#)

**devtools\_not\_connected.js**  
2.5 KB [View](#) [Download](#)

**devtools\_page.html**  
132 bytes [View](#) [Download](#)

**devtools\_page.js**  
4.0 KB [View](#) [Download](#)

**manifest.json**  
222 bytes [View](#) [Download](#)

**notifier.html**  
127 bytes [View](#) [Download](#)

**notifier.js**  
63 bytes [View](#) [Download](#)

Comment 1 by [derce...@gmail.com](#) on Fri, Jul 3, 2020, 12:51 AM EDT

There are three essential requirements for taking advantage of the timing issue present here:

1. You need the user to open the devtools on a non-privileged page. If they've installed a devtools\_page extension, they're probably going to open the devtools and if they're someone like a web developer, they're probably going to be debugging a standard web page.
2. You need to be able to reliably take advantage of the timing issue. Although one of the CLs for [issue-1050577](#) incorporated a test for the timing issue (and the test has since been removed due to flakiness), I think that sort of approach can be intermittent.

If you can send the devtools a message, but delay it from processing that message until after the target page has been navigated to a privileged location, you should be able to reliably sidestep the timing issue.

The method here relies on sending a crafted setSidebarContent message to the devtools. Within the devtools, \_onSetSidebarContent starts with the following code:

```
const sidebar = this._clientObjects[message.id];
```

[https://source.chromium.org/chromium/chromium/src/+master:third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js;\\_id=396;drc=4576282f49d8129b6374dd0fd389271c0a291b6a](https://source.chromium.org/chromium/chromium/src/+master:third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js;_id=396;drc=4576282f49d8129b6374dd0fd389271c0a291b6a)

message.id is something that's controlled by the sending extension. In this case, the extension generates the id as follows:

```
let idArray = new Array(100000);
let innerArray = [];
for (let i = 0; i < 250; i++) {innerArray = [innerArray];}
idArray.fill(innerArray);
```

This array is relatively small and quick to generate. It's then sent to the devtools via the following call:

```
channel.port1.postMessage({command: "setSidebarContent", id: idArray, expression: "...", rootTitle: "Title", evaluateOnPage: true});
```

When the devtools runs the \_clientObjects lookup line of code above, the array will be implicitly converted to a string. That operation takes a non-trivial amount of time to complete (due to the nested arrays). On my machine, it's about 15 seconds. However, the string that's generated is small (about 100 KB), because none of the nested arrays contribute to the final output.

So this gives you an array that's:

- quick to generate,
- reasonably small,
- time consuming to convert to a string,
- small when represented as a string.

The target page is then navigated to a privileged location. Once the devtools is done running the single line of code above, it will continue with the rest of the \_onSetSidebarContent method. Once it's finished calling the method, the navigation change event will be handled.

By doing this, the extension can ensure that the setSidebarContent message is sent to the devtools before the target page is navigated, not fully processed until after navigation has finished, but before the navigation notification is handled.

3. The final requirement has to do with how the devtools handles evaluation requests. Firstly, the evaluate method in ExtensionServer performs several URL checks:

[https://source.chromium.org/chromium/chromium/src/+master:third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js;\\_id=949;drc=4576282f49d8129b6374dd0fd389271c0a291b6a](https://source.chromium.org/chromium/chromium/src/+master:third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js;_id=949;drc=4576282f49d8129b6374dd0fd389271c0a291b6a)

In this case, the URL checks don't matter, because the devtools effectively runs \_onSetSidebarContent before it's handled the navigation change event. That means all of the context and URL information will still be for the previous page (which the extension had access to).

To evaluate code on the target page, the devtools calls the Runtime.evaluate method and passes it the ID of the appropriate context:

[https://source.chromium.org/chromium/chromium/src/+master:third\\_party/devtools-frontend/src/front\\_end/sdk/RuntimeModel.js;\\_id=814;drc=080e864790b3c7fb5265341ed8091cbf8b3d335d7](https://source.chromium.org/chromium/chromium/src/+master:third_party/devtools-frontend/src/front_end/sdk/RuntimeModel.js;_id=814;drc=080e864790b3c7fb5265341ed8091cbf8b3d335d7)

The problem here is that if the context ID on the initial page isn't valid on the privileged page, the call will fail. The extension needs to ensure that the context ID on the original page is also valid for the privileged page.

My understanding is that the context ID gets incremented when there are multiple contexts (for a particular site) within the same process.

I believe that the context ID for the privileged page (in this case devtools://devtools/bundled/inspector.html) will always be 1, because going from a non-privileged page to a privileged page involves switching to a new process.

Ensuring that the context ID on the initial (non-privileged page) is 1 can be done by first navigating the target page from whatever page the user opened to a page that they're likely to have never opened (so that there won't be any other tabs open on that page). The page chosen here is <https://example.com/>, since it's unlikely that the user will have that open in another tab.

Ultimately, this should result in a situation where the context ID of the main frame on the initial page is 1 and ID of the main frame on the privileged page is also 1, which then means the call to Runtime.evaluate will succeed.

Comment 2 by [derce...@gmail.com](#) on Fri, Jul 3, 2020, 12:57 AM EDT

Putting these pieces above together, here's an overview of what happens once the extension is installed:

1. The user opens the devtools on a non-privileged page. The extension downloads the target executable and navigates the page being debugged to <https://example.com/>.
2. The extension creates a sidebar in the devtools by sending the createSidebarPane message.
3. The extension sends the setSidebarContent message to the devtools. The devtools starts processing this message, which will take a non-trivial amount of time.
4. The extension forwards the Alt+R keyboard shortcut to the devtools. As the devtools is busy handling the previous message, this message won't be handled immediately.
5. The extension navigates the page being debugged to devtools://devtools/bundled/inspector.html.
6. Some time later, the devtools finishes processing the setSidebarContent message. As part of that, it will run the expression that was given on the debugged page, which is now a privileged page. The expression that's run results in a console pin being added.
7. The extension will handle the Alt+R shortcut that was forwarded and reload. Although the keyboard shortcut message will always be sent before the navigation notification, I'm not sure if it's guaranteed that the devtools will handle it first. It is possible to perform the same process without reloading the devtools, though it would make the demonstration more complicated.
8. Once the devtools reloads, any embedded extensions will be disabled (since the target is a privileged page), but the console pin that was added in step 6 will run. From this point, the steps are the same as those described in [issue-1067282](#).

Comment 3 by [carlosil@chromium.org](mailto:carlosil@chromium.org) on Mon, Jul 6, 2020, 5:39 PM EDT

Status: Assigned (was: Unconfirmed)

Owner: caseq@chromium.org

Labels: Security\_Impact-Stable Security\_Severity-Medium OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows

Components: Platform>DevTools Platform>Extensions

caseq: Looks like this is an alternate case of what was fixed in [a bug.com/1060677](https://bug.com/1060677). Can you please take a look? Thanks.

Comment 4 by [mea...@chromium.org](mailto:mea...@chromium.org) on Mon, Jul 6, 2020, 7:43 PM EDT

Cc: [dpa...@chromium.org](mailto:dpa...@chromium.org) [tommycli@chromium.org](mailto:tommycli@chromium.org)

+tommycli and dpapad from [bug-1101024](#)

Comment 5 by [derce...@gmail.com](mailto:derce...@gmail.com) on Mon, Jul 6, 2020, 11:46 PM EDT

It is also possible to take advantage of the same issue with the "Reload" method that the devtools makes available to extensions. This method allows an injected script to be run when the page is reloaded:

[https://source.chromium.org/chromium/chromium/src/+master:third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js;l=467;dr=4576282f49d8129b6374dd0fd389271c0a291b6a](https://source.chromium.org/chromium/chromium/src/+master:third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js;l=467;dr=4576282f49d8129b6374dd0fd389271c0a291b6a)

By generating options.injectedScript in the same sort of way as the sidebar ID, the devtools will take a non-trivial amount of time to process that specific line of code. If the target page has been navigated since the message was sent, the injected script will run on the new page (which can be privileged).

The advantage of this method over setSidebarContent is that the extension doesn't have to worry about the context IDs at all. The Reload method (which is ultimately implemented via Page.reload in the devtools protocol) always runs the injected script within the context of the main frame:

[https://source.chromium.org/chromium/chromium/src/+master:third\\_party/blink/renderer/core/inspector/inspector\\_page\\_agent.cc;l=903;dr=8178c4af08c01c3673549f2531953997c74f09b](https://source.chromium.org/chromium/chromium/src/+master:third_party/blink/renderer/core/inspector/inspector_page_agent.cc;l=903;dr=8178c4af08c01c3673549f2531953997c74f09b)

I've attached a small extension here that demonstrates that it's possible to use this method to run code within the context of a privileged page.

To test, install the extension, open the devtools on a non-privileged page, wait about 15 seconds, then check the console for the following message:

Injected script run on: devtools://devtools/bundled/inspector.html

**devtools\_page.html**  
132 bytes [View](#) [Download](#)

**devtools\_page.js**  
1.5 KB [View](#) [Download](#)

**manifest.json**  
165 bytes [View](#) [Download](#)

Comment 6 by [tommycli@chromium.org](mailto:tommycli@chromium.org) on Tue, Jul 7, 2020, 12:29 PM EDT

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

[issue-1101024](#) has been merged into this issue.

Comment 7 by [tommycli@chromium.org](mailto:tommycli@chromium.org) on Tue, Jul 7, 2020, 12:33 PM EDT

Labels: -Security\_Severity-Medium Security\_Severity-High

Based on the explanation I'm reading in c#5, this can be used to run arbitrary JavaScript on chrome://settings.

If true, I'd recommend upgrading to at least High, depending on how easy it is to exploit.

Arbitrary JavaScript running on chrome://settings can steal the user's home address on chrome://settings/addresses. It can also steal users' saved passwords from chrome://settings/passwords.

If this is exploitable by merely installing an extension, I recommend upgrading this to a P0 / Critical.

Comment 8 by [tommycli@chromium.org](mailto:tommycli@chromium.org) on Tue, Jul 7, 2020, 12:34 PM EDT

Cc: [mea...@chromium.org](mailto:mea...@chromium.org)

Comment 9 by [sheriffbot](#) on Tue, Jul 7, 2020, 1:54 PM EDT

Labels: M-83 Target-83

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 10 by [sheriffbot](#) on Tue, Jul 7, 2020, 2:34 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 11 by [mea...@chromium.org](mailto:mea...@chromium.org) on Tue, Jul 7, 2020, 8:49 PM EDT

Per chrome-security chat, [bug-1060677](#) could actually be high severity, so this one could be too. Code execution outside the sandbox is normally critical, but the extension install is a significant mitigation / friction, so we downgrade severity by one notch.

Comment 12 by sheriffbot on Wed, Jul 15, 2020, 1:33 PM EDT

Labels: -M-83 Target-84 M-84

Comment 13 by sheriffbot on Fri, Jul 17, 2020, 1:32 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 14 by rsleevi@chromium.org on Tue, Jul 28, 2020, 1:15 PM EDT

caseq: Friendly ping here as well?

Comment 15 by sheriffbot on Fri, Jul 31, 2020, 1:37 PM EDT

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 caseq@chromium.org on Mon, Aug 24, 2020, 9:37 PM EDT

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

Comment 17 by sheriffbot on Wed, Aug 26, 2020, 1:38 PM EDT

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

Comment 18 by sheriffbot on Tue, Sep 1, 2020, 3:14 PM EDT

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 19 by sheriffbot on Wed, Oct 7, 2020, 1:37 PM EDT

Labels: -M-85 M-86 Target-86

Comment 20 by vakh@chromium.org on Thu, Oct 22, 2020, 12:30 PM EDT

Friendly ping from the security 🐞 for this High severity bug. Any updates?

For high severity vulnerabilities, we aim to deploy the patch to all Chrome users in under 60 days.

Comment 21 by sheriffbot on Fri, Oct 30, 2020, 6:46 PM EDT

Labels: reward-potential

Comment 22 by sheriffbot on Wed, Nov 18, 2020, 12:22 PM EST

Labels: -M-86 M-87 Target-87

Comment 23 by bugdroid on Tue, Dec 22, 2020, 9:06 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+bbf439e4e27540642b4ed172269274d2889c9cd6>

commit bbf439e4e27540642b4ed172269274d2889c9cd6

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Wed Dec 23 02:05:41 2020

DevTools: prepare tests for introduction of ExecutionContextDescription.uniqueId

This temporarily removes the newly added field from objects being dumped, so that the test expectations do not change when upstream CL lands.

Bug: v8:11268, ~~chromium:1104907~~

Change-Id: I8caa2bcf4a5b71250fb0712129771215c3a215bb

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2601547>

Reviewed-by: Peter Kvitsek <kvitek@chromium.org>

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

Cr-Commit-Position: refs/heads/master@{#839032}

[modify] [https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third\\_party/blink/web\\_tests/http/tests/inspector-protocol/mixed-content-execution-contexts-1.js](https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third_party/blink/web_tests/http/tests/inspector-protocol/mixed-content-execution-contexts-1.js)

[modify] [https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third\\_party/blink/web\\_tests/http/tests/inspector-protocol/iframe-no-src-execution-contexts.js](https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third_party/blink/web_tests/http/tests/inspector-protocol/iframe-no-src-execution-contexts.js)

[modify] [https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third\\_party/blink/web\\_tests/http/tests/inspector-protocol/mixed-content-execution-contexts-2.js](https://crrev.com/bbf439e4e27540642b4ed172269274d2889c9cd6/third_party/blink/web_tests/http/tests/inspector-protocol/mixed-content-execution-contexts-2.js)

Comment 24 by bugdroid on Wed, Dec 23, 2020, 12:16 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/v8/v8/+f656eab5928876809ef46e18de0c9d35d489e17a>

commit f656eab5928876809ef46e18de0c9d35d489e17a

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Wed Dec 23 05:15:47 2020

DevTools: add support for system-unique execution context ids

This adds ExecutionContextDescription.uniqueId for a system-unique way to identify an execution context and supports it in Runtime.evaluate. This allows a client to avoid accidentally executing an expression in a context different from that originally intended if a navigation occurs while Runtime.evaluate is in flight.

Design doc: [https://docs.google.com/document/d/1vGVWvKP9FTTX6kmcUJR\\_PAVgDelzXXITFpl0SyghQ](https://docs.google.com/document/d/1vGVWvKP9FTTX6kmcUJR_PAVgDelzXXITFpl0SyghQ)

Bug: v8:11268, [chromium:1104907](#)

Change-Id: I4c6bec562ffc85312559316f639d641780144039

Reviewed-on: <https://chromium-review.googlesource.com/c/v8/v8/+2594538>

Commit-Queue: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

Reviewed-by: Dmitry Gozman <[dgozman@chromium.org](mailto:dgozman@chromium.org)>

Reviewed-by: Benedikt Meurer <[bmeurer@chromium.org](mailto:bmeurer@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#71869}

[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-debugger.cc>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-runtime-agent-impl.h>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-inspector-impl.cc>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-inspector-impl.h>  
[add] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/runtime/evaluate-unique-context-id-expected.txt>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/runtime/runtime-restore-expected.txt>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/protocol-test.js>  
[add] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-debugger-id.h>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/sessions/create-session-expected.txt>  
[add] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-debugger-id.cc>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/BUILD.gn>  
[add] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/runtime/evaluate-unique-context-id.js>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/inspected-context.cc>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/inspected-context.h>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/test/inspector/runtime/create-context-expected.txt>  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-debugger.h>  
[modify] [https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/include/js\\_protocol.pdl](https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/include/js_protocol.pdl)  
[modify] <https://crrev.com/f656eab5928876809ef46e18de0c9d35d489e17a/src/inspector/v8-runtime-agent-impl.cc>

Comment 25 by [bugdroid](#) on Thu, Dec 24, 2020, 12:33 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/devtools/devtools-frontend/+b961d44fa6990b049d82caeac1dc59c1d4be0848>

commit [b961d44fa6990b049d82caeac1dc59c1d4be0848](#)

Author: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

Date: Thu Dec 24 05:30:57 2020

Roll js\_protocol.pdl to include ExecutionContextDescription.uniqueId

Drive-by: roll inspector\_protocol to fix pdl.py problem

DISABLE\_THIRD\_PARTY\_CHECK=protocol update

Bug: v8:11268, [chromium:1104907](#)

Change-Id: I8c0be131e521d996fb718ee381fe67f14dfe737d

Reviewed-on: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2602555>

Reviewed-by: Benedikt Meurer <[bmeurer@chromium.org](mailto:bmeurer@chromium.org)>

Commit-Queue: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

[modify] [https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/front\\_end/generated/InspectorBackendCommands.js](https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/front_end/generated/InspectorBackendCommands.js)  
[modify] [https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/v8/include/js\\_protocol.pdl](https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/v8/include/js_protocol.pdl)  
[modify] [https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/front\\_end/generated/protocol.d.ts](https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/front_end/generated/protocol.d.ts)  
[modify] [https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/third\\_party/blink/public/devtools\\_protocol/browser\\_protocol.json](https://crrev.com/b961d44fa6990b049d82caeac1dc59c1d4be0848/third_party/blink/public/devtools_protocol/browser_protocol.json)

Comment 26 by [bugdroid](#) on Thu, Dec 24, 2020, 12:59 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/devtools/devtools-frontend/+58d64f52a1303ce60ef0e4abe17d0f36c67ebe4a>

commit [58d64f52a1303ce60ef0e4abe17d0f36c67ebe4a](#)

Author: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

Date: Thu Dec 24 05:57:47 2020

Use ExecutionContext.uniqueId when evaluating on the global object

Design doc: [https://docs.google.com/document/d/1vGVWvKP9FTTX6kmcUJR\\_PAVgDelzXXITFpl0SyghQ](https://docs.google.com/document/d/1vGVWvKP9FTTX6kmcUJR_PAVgDelzXXITFpl0SyghQ)

Related test: <https://chromium-review.googlesource.com/c/chromium/src/+2602709>

Bug: v8:11268, [chromium:1104907](#)

Change-Id: I35f8efba4d50ac8bd98e0fce9955af24dda55365

Reviewed-on: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2602710>

Commit-Queue: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

Reviewed-by: Benedikt Meurer <[bmeurer@chromium.org](mailto:bmeurer@chromium.org)>

Auto-Submit: Andrey Kosyakov <[caseq@chromium.org](mailto:caseq@chromium.org)>

[modify] [https://crrev.com/58d64f52a1303ce60ef0e4abe17d0f36c67ebe4a/front\\_end/sdk/RuntimeModel.js](https://crrev.com/58d64f52a1303ce60ef0e4abe17d0f36c67ebe4a/front_end/sdk/RuntimeModel.js)

Comment 27 by [bugdroid](#) on Thu, Dec 24, 2020, 10:55 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+8afc6a72b00f9198409c4ed6ba9df82daab1fb8b>

commit [8afc6a72b00f9198409c4ed6ba9df82daab1fb8b](#)

Author: chromium-autoroll <[chromium-autoroll@skia-public.iam.gserviceaccount.com](mailto:chromium-autoroll@skia-public.iam.gserviceaccount.com)>

Date: Thu Dec 24 15:54:48 2020

Roll DevTools Frontend from b4a82aa3575f to b961d44fa699 (1 revision)

<https://chromium.googlesource.com/devtools/devtools-frontend.git/+log/b4a82aa3575f..b961d44fa699>

2020-12-24 [caseq@chromium.org](mailto:caseq@chromium.org) Roll js\_protocol.pdl to include ExecutionContextDescription.uniqueId

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@rotations.appspotmail.com](mailto:devtools-waterfall-sheriff-onduty@rotations.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=Authoroller+Bug>

Documentation for the AutoRoller is here:

<https://skia.googlesource.com/buildbot/+doc/master/autoroll/README.md>

~~Bug-chromium:1104807~~

Tbr: devtools-waterfall-sheriff-onduty@grotations.appspotmail.com  
Change-Id: Iab489f884fa4ae20dd0c6ceb25c40b00bae25f2a  
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2602835>  
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@{#839264}

[modify] <https://crrev.com/8afc6a72b00f9198409c4ed6ba9df82daab1fb8b/DEPS>

Comment 28 by bugdroid on Thu, Dec 24, 2020, 12:14 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+cbe5f1ae8e69bdfb1be09c65a81db0755e63c356>

commit cbe5f1ae8e69bdfb1be09c65a81db0755e63c356

Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>

Date: Thu Dec 24 17:09:59 2020

Roll DevTools Frontend from b961d44fa699 to fafa67016f36 (19 revisions)

<https://chromium.googlesource.com/devtools/devtools-frontend.git/+log/b961d44fa699..fafa67016f36>

2020-12-24 changhaohan@chromium.org Change cursor to pointer when hovering over color swatches  
2020-12-24 devtools-ci-autoroll-builder@chops-service-accounts.iam.gserviceaccount.com Update DevTools DEPS.  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ElementsSidebarPane.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ComputedStyleWidget.js  
2020-12-24 mathias@chromium.org Use AVIF for "what's new" image  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ComputedStyleModel.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ARIAAttributesView.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ConsolePinPane.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ImagePreview.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in DebuggerWorkspaceBinding.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in TempFile.js  
2020-12-24 mathias@chromium.org Support AVIF in component server  
2020-12-24 mathias@chromium.org Support AVIF in hosted mode  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ClassesPaneWidget.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in WarningErrorCounter.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ConsoleView.js  
2020-12-24 mathias@chromium.org Clean up redundant Promise.resolve() in ContentProviderBasedProject.js  
2020-12-24 devtools-ci-autoroll-builder@chops-service-accounts.iam.gserviceaccount.com Update DevTools Chromium DEPS.  
2020-12-24 caseq@chromium.org Use ExecutionContext.uniqueId when evaluating on the global object

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](mailto: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/+doc/master/autoroll/README.md>

~~Bug-chromium:1104807~~, chromium:1156835, chromium:1161504, chromium:1161664, chromium:1161667

Tbr: devtools-waterfall-sheriff-onduty@grotations.appspotmail.com  
Change-Id: Idfc7cc3c70e50c62eab2aeece3dc2a2f5c0066a  
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2603119>  
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@{#839268}

[modify] <https://crrev.com/cbe5f1ae8e69bdfb1be09c65a81db0755e63c356/DEPS>

Comment 29 by bugdroid on Sat, Dec 26, 2020, 6:55 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+0e3033a6cb7e0283cab92b52f91642eb3cefc888>

commit 0e3033a6cb7e0283cab92b52f91642eb3cefc888

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Sat Dec 26 23:54:37 2020

DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context

See also: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2602710>

Bug: v8:11268, ~~chromium:1104807~~

Change-Id: If57b53a910afe8945453f35689b63168c076db7c  
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2602709>  
Reviewed-by: Benedikt Meurer <bmeurer@chromium.org>  
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>  
Cr-Commit-Position: refs/heads/master@{#839375}

[modify] [https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third\\_party/blink/web\\_tests/http/tests/devtools/resources/extension-main.js](https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third_party/blink/web_tests/http/tests/devtools/resources/extension-main.js)

[add] [https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt](https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt)

[add] [https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js](https://crrev.com/0e3033a6cb7e0283cab92b52f91642eb3cefc888/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js)

Comment 30 by bugdroid on Mon, Dec 28, 2020, 9:41 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+b4db63fc67e6e6b2bf7e36b90dc86b7adf312c50>

commit b4db63fc67e6e6b2bf7e36b90dc86b7adf312c50

Author: Sergey Poromov <poromov@chromium.org>

Date: Mon Dec 28 14:41:20 2020

Revert "DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context"

This reverts commit 0e3033a6cb7e0283cab92b52f91642eb3cefc888.

Reason for revert:

Consistently failing on Linux MSAN builds:

<https://ci.chromium.org/p/chromium/builders/ci/WebKit%20Linux%20MSAN>

First failure: <https://ci.chromium.org/ui/p/chromium/builders/ci/WebKit%20Linux%20MSAN/8844/blamelist>

Original change's description:

> DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context

>

> See also: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2602710>

>

> Bug: v8:11268, ~~chromium:1404807~~

> Change-Id: If57b53a910afe8945453f35689b63168c076db7c

> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2602709>

> Reviewed-by: Benedikt Meurer <bmeurer@chromium.org>

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

> Cr-Commit-Position: refs/heads/master@{#839375}

TBR=caseq@chromium.org,bmeurer@chromium.org,chromium-scoped@luci-project-accounts.iam.gserviceaccount.com,pfaffe@chromium.org

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

Bug: v8:11268

~~Bug-chromium:1404807~~

Change-Id: Ie7aaebbd32400ffa5303774840eb7650c0cc1f4f

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2602428>

Reviewed-by: Sergey Poromov <poromov@chromium.org>

Commit-Queue: Sergey Poromov <poromov@chromium.org>

Cr-Commit-Position: refs/heads/master@{#839449}

[modify] [https://crrev.com/b4db63fc67e6e6b2b7e36b90dc86b7ad312c50/third\\_party/blink/web\\_tests/http/tests/devtools/resources/extension-main.js](https://crrev.com/b4db63fc67e6e6b2b7e36b90dc86b7ad312c50/third_party/blink/web_tests/http/tests/devtools/resources/extension-main.js)

[delete] [https://crrev.com/79b51121c1d96457223e9fb1ab0b1ea253fbe688/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt](https://crrev.com/79b51121c1d96457223e9fb1ab0b1ea253fbe688/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt)

[delete] [https://crrev.com/79b51121c1d96457223e9fb1ab0b1ea253fbe688/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js](https://crrev.com/79b51121c1d96457223e9fb1ab0b1ea253fbe688/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js)

Comment 31 by bugdroid on Mon, Dec 28, 2020, 8:19 PM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+a042444563df9738971aeeb0cd067d89345cbce8>

commit a042444563df9738971aeeb0cd067d89345cbce8

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Tue Dec 29 01:18:52 2020

Reland "DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context"

This reverts commit b4db63fc67e6e6b2b7e36b90dc86b7ad312c50.

Reason for revert: re-land the test along with a fix.

Original change's description:

> Revert "DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context"

>

> This reverts commit 0e3033a6cb7e0283cab92b52f91642eb3cefc888.

>

> Reason for revert:

> Consistently failing on Linux MSAN builds:

> <https://ci.chromium.org/p/chromium/builders/ci/WebKit%20Linux%20MSAN>

> First failure: <https://ci.chromium.org/ui/p/chromium/builders/ci/WebKit%20Linux%20MSAN/8844/blamelist>

>

> Original change's description:

>> DevTools: add a test for chrome.devtools.inspectedWindow.eval using correct execution context

>>

>> See also: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2602710>

>>

>> Bug: v8:11268, ~~chromium:1404807~~

>> Change-Id: If57b53a910afe8945453f35689b63168c076db7c

>> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2602709>

>> Reviewed-by: Benedikt Meurer <bmeurer@chromium.org>

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

>> Cr-Commit-Position: refs/heads/master@{#839375}

>

TBR=caseq@chromium.org,bmeurer@chromium.org,chromium-scoped@luci-project-accounts.iam.gserviceaccount.com,pfaffe@chromium.org

>

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

>

> Bug: v8:11268

> ~~Bug-chromium:1404807~~

> Change-Id: Ibc4e38986ca13bc89b334bb90ea0d6704c5c86a

> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2605411>

> Reviewed-by: Sergey Poromov <poromov@chromium.org>

> Commit-Queue: Sergey Poromov <poromov@chromium.org>

> Cr-Commit-Position: refs/heads/master@{#839449}

TBR=caseq@chromium.org,poromov@chromium.org,bmeurer@chromium.org,chromium-scoped@luci-project-accounts.iam.gserviceaccount.com,pfaffe@chromium.org

# Not skipping CQ checks because this is a reland.

Bug: v8:11268

~~Bug-chromium:1404807~~

Change-Id: Ibc4e38986ca13bc89b334bb90ea0d6704c5c86a

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2605411>

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

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

Cr-Commit-Position: refs/heads/master@{#839521}

[modify] [https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third\\_party/blink/web\\_tests/http/tests/devtools/resources/extension-main.js](https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third_party/blink/web_tests/http/tests/devtools/resources/extension-main.js)

[add] [https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt](https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context-expected.txt)

[add] [https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third\\_party/blink/web\\_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js](https://crrev.com/a042444563df9738971aeeb0cd067d89345cbce8/third_party/blink/web_tests/http/tests/devtools/extensions/extensions-eval-execution-context.js)

Comment 32 by sheriffbot on Wed, Jan 20, 2021, 12:23 PM EST

Labels: -M-87 Target-88 M-88

Comment 33 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST

**Labels:** -reward-potential external\_security\_report

[Comment 34](#) by [sheriffbot](#) on Wed, Mar 3, 2021, 12:22 PM EST

**Labels:** -M-88 Target-89 M-89

[Comment 35](#) by [sheriffbot](#) on Wed, Mar 10, 2021, 8:05 PM EST

**Labels:** reward-potential

[Comment 36](#) by [zhangtiff@google.com](#) on Wed, Mar 17, 2021, 7:12 PM EDT

**Labels:** -reward-potential external\_security\_bug

[Comment 37](#) by [adetaylor@google.com](#) on Thu, Apr 8, 2021, 1:25 PM EDT

[caseq@](#) is this now fixed? I've belatedly noticed that the commit description in [#c31](#) suggests so.

[Comment 38](#) by [bmeu...@chromium.org](#) on Fri, Apr 9, 2021, 4:22 AM EDT

**Cc:** [sigurds@chromium.org](#)

[Comment 39](#) by [sheriffbot](#) on Thu, Apr 15, 2021, 12:23 PM EDT

**Labels:** -M-89 M-90 Target-90

[Comment 40](#) by [Git Watcher](#) on Wed, Apr 21, 2021, 1:24 AM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/devtools/devtools-frontend/+b7e80e33dc247c4bc1d0bef976954c4a70145982>

commit [b7e80e33dc247c4bc1d0bef976954c4a70145982](#)

Author: Benedikt Meurer <[bmeurer@chromium.org](#)>

Date: Wed Apr 21 04:57:27 2021

[sdk] Support old backends that don't understand uniqueContextId.

With <https://crrev.com/c/2602710> we broke support for `Runtime.evaluate()` with different contexts for back-ends that don't yet support `uniqueContextId`. This change restores support by using `uniqueContextId` only when it was send by the back-end and otherwise using `contextId` as before.

~~Fixed: [chromium:1102624](#)~~

~~Bug: [v8:11268](#), [chromium:1101807](#)~~

Change-Id: [I37909443eaea6fb4d92a1c258383a4753639c8b9](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2815125>

Commit-Queue: Benedikt Meurer <[bmeurer@chromium.org](#)>

Auto-Submit: Benedikt Meurer <[bmeurer@chromium.org](#)>

Reviewed-by: Sigurd Schneider <[sigurds@chromium.org](#)>

Reviewed-by: Andrey Kosyakov <[caseq@chromium.org](#)>

[modify] [https://crrev.com/b7e80e33dc247c4bc1d0bef976954c4a70145982/front\\_end/core/sdk/RuntimeModel.ts](https://crrev.com/b7e80e33dc247c4bc1d0bef976954c4a70145982/front_end/core/sdk/RuntimeModel.ts)

[Comment 41](#) by [Git Watcher](#) on Wed, Apr 21, 2021, 4:16 AM EDT

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+5d3026bc75b1f3d681e6d64cc57e38858ab7a400>

commit [5d3026bc75b1f3d681e6d64cc57e38858ab7a400](#)

Author: chromium-autoroll <[chromium-autoroll@skia-public.iam.gserviceaccount.com](#)>

Date: Wed Apr 21 08:15:43 2021

Roll DevTools Frontend from [c8dcfdebd148](#) to [b7e80e33dc24](#) (1 revision)

<https://chromium.googlesource.com/devtools/devtools-frontend.git/+log/c8dcfdebd148..b7e80e33dc24>

2021-04-21 [bmeurer@chromium.org](#) [sdk] Support old backends that don't understand uniqueContextId.

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/+doc/master/autoroll/README.md>

~~Bug: [chromium:1101807](#)~~

Tbr: [devtools-waterfall-sheriff-onduty@grotations.appspotmail.com](#)

Change-Id: [I569d522cd9d0d0804038507023fde045e7463121](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2843269>

Commit-Queue: chromium-autoroll <[chromium-autoroll@skia-public.iam.gserviceaccount.com](#)>

Bot-Commit: chromium-autoroll <[chromium-autoroll@skia-public.iam.gserviceaccount.com](#)>

Cr-Commit-Position: refs/heads/master@{[#874613](#)}

[modify] <https://crrev.com/5d3026bc75b1f3d681e6d64cc57e38858ab7a400/DEPS>

[Comment 42](#) by [sheriffbot](#) on Wed, May 26, 2021, 12:24 PM EDT

**Labels:** -M-90 M-91 Target-91

[Comment 43](#) by [adetaylor@google.com](#) on Thu, Jul 8, 2021, 4:27 PM EDT

**Labels:** FoundIn-83

[Comment 44](#) by [amyressler@chromium.org](#) on Mon, Jul 19, 2021, 4:27 PM EDT

**Labels:** Release-0-M92

[Comment 45](#) by [amyressler@google.com](#) on Mon, Jul 19, 2021, 7:15 PM EDT

**Labels:** CVE-2021-30571 CVE\_description-missing

[Comment 46](#) by [amyressler@google.com](#) on Tue, Jul 20, 2021, 5:29 PM EDT



Hi, caseq@ and bmeurer@, can this be marked as fixed or are additional fixes needed due to the revert above?

[Comment 47](#) by [amyressler@google.com](#) on Tue, Jul 20, 2021, 5:30 PM EDT

**Labels:** -Release-0-M92

[Comment 48](#) by [caseq@chromium.org](#) on Tue, Jul 20, 2021, 5:31 PM EDT

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

[Comment 49](#) by [amyressler@google.com](#) on Tue, Jul 20, 2021, 5:35 PM EDT

**Labels:** Release-0-M92

[Comment 50](#) by [sheriffbot](#) on Wed, Jul 21, 2021, 12:42 PM EDT

**Labels:** reward-topanel

[Comment 51](#) by [sheriffbot](#) on Wed, Jul 21, 2021, 1:42 PM EDT

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

[Comment 52](#) by [sheriffbot](#) on Sat, Jul 24, 2021, 9:10 AM EDT

**Labels:** Merge-na Merge-Request-91

Requesting merge to extended stable M91 because latest trunk commit (874613) appears to be after extended stable branch point (870763).

Not requesting merge to stable (M92) because latest trunk commit (874613) appears to be prior to stable branch point (885287). If this is incorrect, please replace the Merge-na label with Merge-Request-92. If other changes are required to fix this bug completely, please request a merge if necessary.

Not requesting merge to dev (M93) because latest trunk commit (874613) appears to be prior to dev branch point (902210). If this is incorrect, please replace the Merge-na label with Merge-Request-93. If other changes are required to fix this bug completely, please request a merge if necessary.

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

[Comment 53](#) Deleted

[Comment 54](#) by [amyressler@google.com](#) on Mon, Jul 26, 2021, 3:07 PM EDT

Please ensure the changes from this rollback are included/merged in M91 as it is now the extended stable release branch as we move toward the 4W release cycle. Thanks!

[Comment 55](#) by [caseq@chromium.org](#) on Mon, Jul 26, 2021, 3:15 PM EDT

FWIW, this is not a rollback.

Please note [comment 52](#) refers to the commit that was fixing a regression resulting from the original fix of this issue, which is tracked separately by [issue-1102624](#) -- let's rather track the merge there. The last commit related to the original fix for this issue is landed in m89 (<https://storage.googleapis.com/chromium-find-releases-static/a04.html#a042444563df9738971aeeb0cd067d89345cbce8>)

Benedikt, does it look like something that we'd like to merge to m91 extended stable? My take is that considering we did not do any merges originally and that this is not a security issue, we don't have to.

[Comment 56](#) by [adetaylor@google.com](#) on Tue, Jul 27, 2021, 4:14 AM EDT

**Labels:** -Merge-Approved-91

I agree; removing merge request.

[Comment 57](#) by [amyressler@google.com](#) on Wed, Jul 28, 2021, 4:50 PM EDT

**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-vp@chromium.org](mailto:security-vp@chromium.org) with any questions.

[Comment 58](#) by [amyressler@google.com](#) on Wed, Jul 28, 2021, 4:56 PM EDT

Hi, David! The VRP Panel has decided to award you \$5000 for this report. Also, thank you for your patience as this one ducked some of our automation and was only recently noticed to be left open long after it was fixed. Our apologies for that and thank you for another great report.

[Comment 59](#) by [amyressler@google.com](#) on Thu, Jul 29, 2021, 6:03 PM EDT

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

[Comment 60](#) by [voit@google.com](#) on Mon, Aug 2, 2021, 11:38 PM EDT

**Labels:** LTS-Security-90 LTS-Security-NotApplicable-90

Marking as not applicable for Its. The security issue was fixed in m89, so we don't need to merge anything to m90.

[Comment 61](#) by [amyressler@google.com](#) on Tue, Aug 3, 2021, 3:41 PM EDT

**Labels:** -CVE\_description-missing CVE\_description-submitted

[Comment 62](#) by [sheriffbot](#) on Sat, Oct 30, 2021, 1:30 PM EDT

**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