




☆ Starred by 2 users

Owner:	<a href="#">caseq@chromium.org</a>
CC:	<a href="#">aerot...@chromium.org</a> <a href="#">gov...@chromium.org</a> <a href="#">adetaylor@chromium.org</a> <a href="#">bmeu...@chromium.org</a>  <a href="#">lucferron@chromium.org</a>  <a href="#">hablich@chromium.org</a> <a href="#">pbomm...@chromium.org</a> <a href="#">caseq@chromium.org</a> <a href="#">tvand...@chromium.org</a> <a href="#">mathias@chromium.org</a> <a href="#">solomonkinard@chromium.org</a> <a href="#">tjudkins@chromium.org</a>  <a href="#">dsv@google.com</a>
Status:	Fixed ( <i>Closed</i> )
Components:	<a href="#">Platform&gt;DevTools</a> <a href="#">Platform&gt;Extensions</a>
Modified:	Jul 16, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	<a href="#">Linux, Windows, Chrome, Mac, Fuchsia</a>
Pri:	1
Type:	<a href="#">Bug-Security</a>
<a href="#">Hotlist-Merge-Review</a> <a href="#">reward-3000</a> <a href="#">Security_Impact-Stable</a> <a href="#">Security_Severity-Medium</a> <a href="#">allpublic</a> <a href="#">reward-inprocess</a> <a href="#">CVE_description-submitted</a> <a href="#">M-81</a> <a href="#">Target-81</a> <a href="#">Release-0-M83</a> <a href="#">CVE-2020-6472</a>	

Issue 1064519: Security: DevTools doesn't fully validate channel messages it receives

Reported by [derce...@gmail.com](#) on Wed, Mar 25, 2020, 1:23 AM EDT

 Code

VULNERABILITY DETAILS

When an extension specifies a devtools\_ page entry, a message channel is used behind the scenes to provide the associated API functionality. The DevTools doesn't fully validate messages it receives in this way, allowing an extension to run code within the DevTools context by sending the appropriate messages.

This then allows an extension to access local files and run code within the context of other extensions, without any user interaction (as described in [issue-1050676](#)). If the "debugger" permission is also set, it's also possible to run an executable outside of the sandbox, again without any user interaction (as described in [issue-1050677](#)).

VERSION

Chrome Version: Tested on 80.0.3987.149 (stable) and 83.0.4094.0 (canary)  
Operating System: Windows 10, version 1909

REPRODUCTION CASE

1. Install the attached extension. Ensure "Allow access to file URLs" isn't set.
2. Once loaded, the extension opens a tab at the following location:

`devtools://devtools/bundled/inspector.html`

3. As this page shows a devtools window (though it's not connected to anything), the location specified in the devtools\_ page property is loaded within an iframe.

The extension page that's loaded sends several crafted messages to the DevTools window (via a message channel that's set up). This ultimately allows the extension to run code within the context of the DevTools window.

To demonstrate that this process has succeeded, the extension performs the same steps as those described in [issue-1050676](#) to:

- Open a new tab containing the contents of file:///C:/.
- Disable safe browsing.

CREDIT INFORMATION

Reporter credit: David Erceg

background.js

72 bytes [View](#) [Download](#)

devtools.js

927 bytes [View](#) [Download](#)

devtools\_page.html

132 bytes [View](#) [Download](#)

devtools\_page.js

3.3 KB [View](#) [Download](#)

manifest.json

220 bytes [View](#) [Download](#)

Comment 1 by derce...@gmail.com on Wed, Mar 25, 2020, 1:31 AM EDT

The core issue here is that the DevTools doesn't completely validate channel messages it receives from an untrusted extension renderer. Specifically, `_onAddRequestHeaders` allows certain properties to be overwritten:

[https://cs.chromium.org/chromium/src/third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js?l=231&rc1=98583637e9c4901ed5587a65b5992668e705b15f](https://cs.chromium.org/chromium/src/third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js?l=231&rc1=98583637e9c4901ed5587a65b5992668e705b15f)

This function updates values in `_extraHeaders` in the following way:

```
const id = message.extensionId;
let extensionHeaders = this._extraHeaders[id];
for (const name in message.headers) {
  extensionHeaders[name] = message.headers[name];
}
```

This is potentially dangerous, as the `id` field is completely controlled by the extension and can take any value. This code means that, for example, it's possible to set or overwrite values on `_extraHeaders["__proto__"]` (i.e. `Object.prototype`).

The extension in the demonstration takes advantage of this to assign a port to `Object.prototype["0"]`:

```
standardChannel.port1.postMessage({
  command: "addRequestHeaders",
  headers: {"0": controlledChannel.port2},
  extensionId: "__proto__"
}, [controlledChannel.port2]);
```

Next, the extension calls `registerExtension`:

```
parent.postMessage("registerExtension", "");
```

This message typically requires a port to be supplied:

[https://cs.chromium.org/chromium/src/third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js?l=774&rc1=98583637e9c4901ed5587a65b5992668e705b15f](https://cs.chromium.org/chromium/src/third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js?l=774&rc1=98583637e9c4901ed5587a65b5992668e705b15f)

However, because `Object.prototype["0"]` was set above, `event.ports[0]` will ultimately refer to that. This means that the DevTools will start listening for messages on `controlledChannel.port2`.

The extension can then make another `addRequestHeaders` call to overwrite the `_extensionOrigin` property that's set on the target port by `_registerExtension`:

[https://cs.chromium.org/chromium/src/third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js?l=767&rc1=98583637e9c4901ed5587a65b5992668e705b15f](https://cs.chromium.org/chromium/src/third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js?l=767&rc1=98583637e9c4901ed5587a65b5992668e705b15f)

```
let scriptUrl = chrome.extension.getURL("devtools.js");
let extensionOrigin = `javascript:let script = document.createElement("script");script.src = "${scriptUrl}";document.head.appendChild(script);`;
controlledChannel.port1.postMessage({
  command: "addRequestHeaders",
  headers: {"_extensionOrigin": extensionOrigin},
  extensionId: "0"
});
```

This is important, as the `_extensionOrigin` field is used to build the complete path to an extension resource. For example, the field is used when creating a panel:

[https://cs.chromium.org/chromium/src/third\\_party/devtools-frontend/src/front\\_end/extensions/ExtensionServer.js?l=286&rc1=98583637e9c4901ed5587a65b5992668e705b15f](https://cs.chromium.org/chromium/src/third_party/devtools-frontend/src/front_end/extensions/ExtensionServer.js?l=286&rc1=98583637e9c4901ed5587a65b5992668e705b15f)

At this point, the extension has a port that's registered with the DevTools, but has a custom `_extensionOrigin` value. Therefore, the extension uses this port to create and show a panel, which results in the javascript: URL above being loaded in the DevTools window.

An extension can ultimately use this behavior to perform the same steps as those listed in issues [4050577](#) and [4050676](#). The difference here is in how the behavior is triggered.

Comment 2 by jdeblasio@chromium.org on Wed, Mar 25, 2020, 12:03 PM EDT Project Member

**Status:** Assigned (was: Unconfirmed)

**Owner:** yangguo@chromium.org

**Cc:** caseq@chromium.org

**Labels:** Security\_Impact-Stable Security\_Severity-Medium OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1

**Components:** Platform>DevTools Platform>Extensions

yangguo@: can you take a look at this? Feel free to re-allocate as necessary. Thanks!

cc'ing caseq@ because of his related bugs.

Comment 3 by yangguo@chromium.org on Wed, Mar 25, 2020, 12:20 PM EDT Project Member

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

Comment 4 by bmeu...@chromium.org on Thu, Mar 26, 2020, 4:55 AM EDT Project Member

**Cc:** aerot...@chromium.org tvand...@chromium.org hablich@chromium.org mathias@chromium.org

Looping in a couple of DevTools folks, please have a look at the explanation. TBH I don't know what the threat model is for extensions. My assumption is that DevTools extensions already run with super powers, and that's on purpose.

Comment 5 by mathias@chromium.org on Thu, Mar 26, 2020, 5:13 AM EDT Project Member

**Cc:** lucferron@chromium.org

lucferron@, could you please clarify the threat model for Extensions?

Comment 6 by tvand...@chromium.org on Thu, Mar 26, 2020, 6:51 AM EDT Project Member

I am not sure about the threat model of Extensions either. However, we can resolve this issue anyways by using a 'Map' rather than using objects for lookup. E.g. 'map.set(key, value)'. I think that is a worthwhile change for readability as well.

Comment 7 by sheriffbot on Thu, Mar 26, 2020, 1:00 PM EDT Project Member

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

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 8 by bugdroid on Wed, Apr 1, 2020, 6:52 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/devtools/devtools-frontend/+4d123409dc1a1bf42337c9435d0a0aa5af3bfe73>

commit 4d123409dc1a1bf42337c9435d0a0aa5af3bfe73

Author: Andrey Kosyakov <caseq@chromium.org>

Date: Wed Apr 01 22:51:50 2020

Improve code hygiene in ExtensionServer

~~Bug-1064540~~

Change-Id: I9f51bf78a36cf4e96e591d32ed741625f072af06

Reviewed-on: <https://chromium-review.googlesource.com/c/devtools/devtools-frontend/+2131611>

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

Reviewed-by: Tim van der Lippe <tvanterlippe@chromium.org>

[modify] [https://crrev.com/4d123409dc1a1bf42337c9435d0a0aa5af3bfe73/front\\_end/extensions/ExtensionServer.js](https://crrev.com/4d123409dc1a1bf42337c9435d0a0aa5af3bfe73/front_end/extensions/ExtensionServer.js)

Comment 9 by bugdroid on Thu, Apr 2, 2020, 2:55 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+67fd81d2f51379aa9e89be61863b6f213524225c>

commit 67fd81d2f51379aa9e89be61863b6f213524225c

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

Date: Thu Apr 02 06:54:10 2020

Roll src/third\_party/devtools-frontend/src 0a34c98ea0b0..4d123409dc1a (2 commits)

<https://chromium.googlesource.com/devtools/devtools-frontend.git/+log/0a34c98ea0b0..4d123409dc1a>

git log 0a34c98ea0b0..4d123409dc1a --date=short --first-parent --format="%ad %ae %s"

2020-04-01 caseq@chromium.org Improve code hygiene in ExtensionServer

2020-04-01 caseq@chromium.org Disable extensions when inspecting DOM UI

Created with:

gclient setdep -r src/third\_party/devtools-frontend/src@4d123409dc1a

If this roll has caused a breakage, revert this CL and stop the roller

using the controls here:

<https://autoroll.skia.org/r/devtools-frontend-chromium>

Please CC [devtools-waterfall-sheriff-onduty@grotations.appspotmail.com](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/+master/autoroll/README.md>

~~Bug-chromium-1060677, chromium-1064540, chromium-706606~~

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

Change-Id: I9b945356218e8de1b56c79f9b114606beab046d5

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2133415>

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

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

Cr-Commit-Position: refs/heads/master@{#75721}

[modify] <https://crrev.com/67fd81d2f51379aa9e89be61863b6f213524225c/DEPS>

Comment 10 by sheriffbot on Thu, Apr 9, 2020, 12:27 PM EDT Project Member

yangguo: Uh oh! This issue still open and hasn't been updated in the last 15 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 11 by caseq@chromium.org on Thu, Apr 9, 2020, 12:28 PM EDT Project Member

Status: Fixed (was: Assigned)

Owner: caseq@chromium.org

Comment 12 by sheriffbot on Thu, Apr 9, 2020, 2:07 PM EDT Project Member

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

Comment 13 by natashapabrai@google.com on Mon, Apr 13, 2020, 2:37 PM EDT Project Member

Labels: reward-topanel

Comment 14 by sheriffbot on Wed, Apr 15, 2020, 3:27 PM EDT Project Member

Labels: Merge-Request-81

Requesting merge to beta M81 because latest trunk commit (755721) appears to be after beta branch point (737173).

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

Comment 15 by sheriffbot on Wed, Apr 15, 2020, 3:29 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 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](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), geohsu@(ChromeOS), pbommana@(Desktop)

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

[Comment 16](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Apr 15, 2020, 6:50 PM EDT Project Member

**Labels:** -reward-topanel reward-unpaid reward-3000

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

\*\*\*\*\*

[Comment 17](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Apr 15, 2020, 6:54 PM EDT Project Member

Congrats! The Panel decided to award you \$3,000 for this report!

[Comment 18](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Apr 15, 2020, 6:56 PM EDT Project Member

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

[Comment 19](#) by [pbommana@google.com](mailto:pbommana@google.com) on Thu, Apr 16, 2020, 7:31 PM EDT Project Member

**Cc:** [adetaylor@chromium.org](mailto:adetaylor@chromium.org) [pbomm...@chromium.org](mailto:pbomm...@chromium.org) [gov...@chromium.org](mailto:gov...@chromium.org)

[caseq@](#) please reply to [comment#15](#).

+Adetaylor(Security TPM) for approval.

[Comment 20](#) by [caseq@chromium.org](mailto:caseq@chromium.org) on Thu, Apr 16, 2020, 8:10 PM EDT Project Member

**Labels:** -Merge-Review-81

Ah, sorry -- I thought we decided not to merge fixes to another issue with a very similar impact ([issue-1050676](#)), so there's probably no point in merging this one either. Removing Merge-Review labels for the time being, but feel free to bring it back if you thing we should merge this.

[Comment 21](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Thu, Apr 16, 2020, 8:28 PM EDT Project Member

Happy to go with your judgement here, thanks.

[Comment 22](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, May 15, 2020, 3:55 PM EDT Project Member

**Labels:** Release-0-M83

[Comment 23](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, May 18, 2020, 11:58 AM EDT Project Member

**Labels:** CVE-2020-6472 CVE\_description-missing

[Comment 24](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, May 20, 2020, 11:43 PM EDT Project Member

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

[Comment 25](#) by [sheriffbot](#) on Thu, Jul 16, 2020, 3:03 PM EDT Project Member

**Labels:** -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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