



chromium ▾

New issue

Open issues ▾

🔍 Search chromium issue ▾ ⚙️




Sign in

★ Starred by 3 users

Owner:

dsv@chromium.org

CC:

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

Status:

Fixed (*Closed*)

Components:

[Platform>DevTools](#)
[Platform>Extensions](#)

Modified:

Aug 1, 2022

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

[Windows](#)

Pri:

1

Type:

[Bug-Security](#)

M-100
reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-88
Target-85
Target-86
Target-87
Target-89
Target-90
FoundIn-84
Target-91
Target-92
external_security_report
Target-94
Target-93
external_security_bug
Target-96
Target-98
Target-100



Issue 1116450: Security: Extensions can capture contents of local files using

Page.captureScreenshot with fromSurface set to false

Reported by [derce...@gmail.com](#) on Fri, Aug 14, 2020, 10:17 AM EDT

Code

VULNERABILITY DETAILS

When using the chrome.debugger API, one of the methods an extension can call is Page.captureScreenshot. That method allows a screenshot of the frame being debugged to be captured.

When the fromSurface parameter passed to that method is set to false, the screenshot is captured from the view, rather than the surface. One consequence of that is that any content drawn on top of the debugged frame will be captured in the screenshot.

An extension can use that fact to capture the contents of local files.

VERSION

Chrome Version: Tested on 84.0.4147.125 (stable) and 86.0.4233.0 (canary)

Operating System: Windows 10, version 1909

REPRODUCTION CASE

1. Install the attached extension. Ensure that "Allow access to file URLs" isn't checked.
2. Once installed, the extension will download local_file.html.
3. Once the download has completed, the extension will open local_file.html in a new tab.
4. local_file.html contains two subframes: one that loads file:///c:/ and another that loads iframe.html from within the extension. Because the second frame has an absolute position, it will be drawn underneath the first frame.
5. The extension will then attach the debugger to iframe.html and call Page.captureScreenshot with fromSurface set to false.
6. Once the extension has received the screenshot data, it will make the following call:

```
chrome.tabs.create({url: "data:image/png;base64," + screenshotData});
```

The resulting tab should show that the contents of the file:///c:/ frame have been captured. This is true even though the file:///c:/ frame is a sibling of the captured frame and not contained within it.

This issue is similar to [issue 1116444](#), which also uses Page.captureScreenshot.

CREDIT INFORMATION

Reporter credit: David Erceg

background.js

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

iframe.html

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

iframe.js

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

local_file.html

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

manifest.json

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

[Comment 1](#) by [vakh@chromium.org](#) on Sat, Aug 15, 2020, 3:56 AM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: caseq@chromium.org

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

Labels: Security_Impact-Stable Security_Severity-Medium OS-Windows

Components: Platform>Extensions Platform>DevTools

1116444, 1116450 are similar to 1113565 so assigning to caseq@ and adding some other folks as well.

[Comment 2](#) by [sheriffbot](#) on Sat, Aug 15, 2020, 2:12 PM EDT Project Member

Labels: Target-85 M-85

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

[Comment 3](#) by [sheriffbot](#) on Sat, Aug 15, 2020, 2:48 PM EDT Project Member

Labels: Pri-1

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

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

[Comment 4](#) by [sheriffbot](#) on Fri, Aug 28, 2020, 1:37 PM EDT Project Member

caseq: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

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

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

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

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

[Comment 5](#) by [sheriffbot](#) on Fri, Sep 11, 2020, 1:37 PM EDT Project Member

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 6 by [sheriffbot](#) on Wed, Oct 7, 2020, 1:37 PM EDT Project Member

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

Comment 7 by [sheriffbot](#) on Fri, Oct 30, 2020, 6:46 PM EDT Project Member

Labels: reward-potential

Comment 8 by [sheriffbot](#) on Wed, Nov 18, 2020, 12:22 PM EST Project Member

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

Comment 9 by [sheriffbot](#) on Wed, Jan 20, 2021, 12:22 PM EST Project Member

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

Comment 10 by [adetaylor@google.com](#) on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 11 by [sheriffbot](#) on Wed, Mar 3, 2021, 12:22 PM EST Project Member

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

Comment 12 by [sheriffbot](#) on Wed, Mar 10, 2021, 8:04 PM EST Project Member

Labels: reward-potential

Comment 13 by [zhangtiff@google.com](#) on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

Labels: -reward-potential external_security_bug

Comment 14 by [sheriffbot](#) on Thu, Apr 15, 2021, 12:23 PM EDT Project Member

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

Comment 15 by [sheriffbot](#) on Wed, May 26, 2021, 12:24 PM EDT Project Member

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

Comment 16 by [adetaylor@google.com](#) on Thu, Jul 8, 2021, 4:33 PM EDT Project Member

Labels: FoundIn-84

Comment 17 by [sheriffbot](#) on Thu, Aug 5, 2021, 1:43 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 18 by [sheriffbot](#) on Fri, Aug 6, 2021, 12:23 PM EDT Project Member

Labels: -Security_Impact-Extended

[Comment 19](#) by [sheriffbot](#) on Fri, Aug 6, 2021, 12:28 PM EDT Project Member

Labels: Security_Impact-Extended

[Comment 20](#) by [sheriffbot](#) on Fri, Aug 6, 2021, 1:30 PM EDT Project Member

Labels: -Security_Impact-Extended Security_Impact-Stable

[Comment 21](#) by [sheriffbot](#) on Sat, Aug 7, 2021, 12:23 PM EDT Project Member

Labels: -M-91 Target-92 M-92

[Comment 22](#) by [sheriffbot](#) on Mon, Aug 16, 2021, 1:14 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

[Comment 23](#) by [sheriffbot](#) on Sat, Sep 11, 2021, 12:23 PM EDT Project Member

Labels: -M-92 M-93 Target-93

[Comment 24](#) by [caseq@chromium.org](#) on Mon, Sep 13, 2021, 11:16 AM EDT Project Member

Status: Duplicate (was: Assigned)

This had the same underlying cause as [Issue 1116444](#) and has been addressed along with that one in <https://chromium-review.googlesource.com/c/chromium/src/+2584806>

The exploit currently fails with:

Unchecked runtime.lastError: {"code":-32000,"message":"Command can only be executed on top-level targets"}

[Comment 25](#) by [caseq@chromium.org](#) on Mon, Sep 13, 2021, 11:16 AM EDT Project Member

Mergedinto: [1116444](#)

[Comment 26](#) by [derce...@gmail.com](#) on Mon, Sep 13, 2021, 11:36 PM EDT

I don't think this issue is a duplicate. While the original demonstration extension does now fail because it's attempting to call `Page.captureScreenshot` for a nested frame, it's simple enough to adjust the extension so that it calls `Page.captureScreenshot` on a top-level frame, but still captures the contents of a local file.

I've attached an updated extension here that demonstrates that. To test:

1. Install the attached extension. Ensure that "Allow access to file URLs" isn't checked.
2. Once installed, the extension will open two new tabs: one containing `manifest.json` and one containing `file:///c:/`.
3. The extension will then attach the debugger to the `manifest.json` tab and call `Page.captureScreenshot` with `fromSurface` set to `false`.
4. Immediately after making that call, the extension will mark the `file:///c:/` tab as active.
5. Once the extension has received the screenshot data, it will make the following call:

```
chrome.tabs.create({url: "data:image/png;base64," + screenshotData});
```

The resulting tab should show that the contents of the `file:///c:/` tab have been captured (along with the rest of the browser window). This is true even though the extension isn't attached to the `file:///c:/` tab.

background.js

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

manifest.json

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

[Comment 27](#) by [derce...@gmail.com](#) on Mon, Sep 13, 2021, 11:40 PM EDT

I think the specific reason the behavior described in the previous comment occurs is because there's a delay (of 1/6th of a second) when capturing a screenshot from the view:

https://source.chromium.org/chromium/chromium/src/+master:content/browser/renderer_host/render_widget_host_impl.cc;l=3356;drc=279d90cbebb0be2bff181c693e6c06cb4ac0f3e8

During that delay, if another tab is made active, the screenshot will ultimately show the contents of that tab, rather than the tab being debugged.

I think the fact that the screenshot is captured from the OS-level window is also part of it, since it means that whatever is shown within that window at the time is what will be captured, regardless of whether that's the original tab or another tab.

[Comment 28](#) by [ajgo@google.com](#) on Thu, Sep 16, 2021, 2:31 PM EDT Project Member

Status: Available (was: Duplicate)

caseq: (security marshal here) could you re-evaluate if this is a duplicate following [comment 27](#) - thanks

[Comment 29](#) by [caseq@chromium.org](#) on Thu, Sep 16, 2021, 6:54 PM EDT Project Member

Status: Assigned (was: Available)

Thanks for the new exploit, David, I'll take a look into this!

[Comment 30](#) by [sheriffbot](#) on Wed, Sep 22, 2021, 12:24 PM EDT Project Member

Labels: -M-93 Target-94 M-94

[Comment 31](#) by [sheriffbot](#) on Mon, Nov 15, 2021, 12:24 PM EST Project Member

Labels: -M-94 Target-96 M-96

[Comment 32](#) by [sheriffbot](#) on Wed, Feb 2, 2022, 12:24 PM EST Project Member

Labels: -M-96 M-98 Target-98

[Comment 33](#) by [sheriffbot](#) on Wed, Mar 30, 2022, 12:24 PM EDT Project Member

Labels: -M-98 M-100 Target-100

[Comment 34](#) by [dsv@chromium.org](#) on Wed, Apr 20, 2022, 11:59 AM EDT Project Member

I wonder what use case do chrome extensions have to capture screenshots not from the surface?
Can we only allow capturing from the surface for extensions?

[Comment 35](#) by [dsv@chromium.org](#) on Fri, Apr 22, 2022, 9:44 AM EDT Project Member

Owner: dsv@chromium.org

[Comment 36](#) by [Git Watcher](#) on Mon, Apr 25, 2022, 8:19 AM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+2e8037c888191e014f208393af3a5bf5da4f83df>

commit [2e8037c888191e014f208393af3a5bf5da4f83df](#)

Author: Danil Somsikov <dsv@chromium.org>

Date: Mon Apr 25 12:18:01 2022

Only allow capturing screenshots from surface for chrome extensions.

[Bug- 1116450](#)

Change-Id: Ia4e081dbd44e0d3e2f85248b9e4ec9306e3ceb72

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3599349>

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

Auto-Submit: Danil Somsikov <dsv@chromium.org>

Commit-Queue: Danil Somsikov <dsv@chromium.org>

Cr-Commit-Position: refs/heads/main@{#995663}

[modify]

https://crrev.com/2e8037c888191e014f208393af3a5bf5da4f83df/content/browser/devtools/protocol/page_handler.cc

[modify]

https://crrev.com/2e8037c888191e014f208393af3a5bf5da4f83df/content/browser/devtools/protocol/devtools_protocol_browser_test.cc

[modify] https://crrev.com/2e8037c888191e014f208393af3a5bf5da4f83df/content/browser/devtools/protocol/page_handler.h

[modify]

https://crrev.com/2e8037c888191e014f208393af3a5bf5da4f83df/content/browser/devtools/render_frame_devtools_agent_host.cc

Comment 37 by [dsv@chromium.org](#) on Mon, Apr 25, 2022, 8:26 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 38 by [sheriffbot](#) on Mon, Apr 25, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 39 by [sheriffbot](#) on Mon, Apr 25, 2022, 1:43 PM EDT Project Member

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

Comment 40 by [amyressler@google.com](#) on Fri, May 6, 2022, 11:19 AM 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 with any questions.

[Comment 41](#) by amyressler@chromium.org on Fri, May 6, 2022, 11:36 AM EDT Project Member

Thank you for this report, David! Due to the mitigations of this issue requiring an installed extension and the user gesture required to trigger this information leak issue, the VRP Panel has decided to award you \$3,000 for this report. Thank you for another detailed report and taking the time to report this issue to us - including catching it still reproduced and providing a secondary POC!

[Comment 42](#) by amyressler@google.com on Fri, May 6, 2022, 9:39 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 43](#) by amyressler@chromium.org on Tue, Jun 21, 2022, 11:53 AM EDT Project Member

Labels: Release-0-M103

[Comment 44](#) by amyressler@google.com on Tue, Jun 21, 2022, 12:56 PM EDT Project Member

Labels: CVE-2022-2160 CVE_description-missing

[Comment 45](#) by amyressler@chromium.org on Fri, Jul 29, 2022, 5:46 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 46](#) by [sheriffbot](#) on Mon, Aug 1, 2022, 1:31 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