


☆ Starred by 1 user


Owner:

toyoshim@chromium.org


CC:




 yhirano@chromium.org



 kinuko@chromium.org



 dharani@chromium.org



 achuith@chromium.org

Status:

Fixed (Closed)

Components:

[Blink>SecurityFeature](#)

[Blink>Loader](#)

[Blink>SecurityFeature>CORS](#)

Modified:

Mar 19, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

[Linux](#), [Android](#), [Windows](#), [Chrome](#), [Mac](#), [Fuchsia](#)

Pri:

2

Type:

[Bug-Security](#)

Reward-1000
Security_Severity-Low
Security_Impact-Stable
Hotlist-Merge-Approved
allpublic
reward-inprocess
CVE_description-submitted
M-79
FoundIn-79
FoundIn-80
merge-merged-3987
merge-merged-80
Release-0-M80
CVE-2020-6408

Issue 1026546: Security: Steal any local picture when open a local html file
Reported by tiebu...@gmail.com on Wed, Nov 20, 2019, 4:30 AM EST

🔗 Code

VULNERABILITY DETAILS

When open a local evil .html file(file://pic_path)), the local picture can be sent to an evil server.

In the stable version,the picture form the file:// domain treats as a tainted canvases.So it causes a console error : "Uncaught DOMException: Failed to execute 'toDataURL' on 'HTMLCanvasElement': Tainted canvases may not be exported."

However, in the latest dev version, the picture from the file domain can be exported with 'toDataURL'. As a result, the base64 code of this picture can be sent to a evil server.

VERSION

Chrome Version: Version 80.0.3973.0 (Developer Build) (64-bit)
Operating System: [Windows10 1909]

Test version:

```
{
  "kind": "storage#object",
  "name": "win32-release_x64/asan-win32-release_x64-716878.zip",
  "size": "1539163928",
  "mediaLink": "https://www.googleapis.com/download/storage/v1/b/chromium-browser-asan/o/win32-release_x64%2Fasan-win32-release_x64-716878.zip?generation=1574231960381428&alt=media",
  "metadata": {
    "cr-commit-position": "refs/heads/master@{#716878}",
    "cr-commit-position-number": "716878",
    "cr-git-commit": "763b7d5ba7a01435a06eccc40f3692ff534471"
  },
  "updated": "2019-11-20T06:39:20.381Z"
}
```

REPRODUCTION CASE

1. Open the server.py with python3. This evil server is used to receive the picture.
2. set the an existing picture path in the poc.html
3. Open the poc.html(file://path/poc.html) with the latest dev chromium.

The picture will be sent to the evil server.

poc.html
1.2 KB [View](#) [Download](#)

server.py
1.6 KB [View](#) [Download](#)

Status: Assigned (was: Unconfirmed)
Owner: toyoshim@chromium.org
Labels: Security_Severity-Low Security_Impact-Head OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Blink>SecurityFeature

Nice find! Bisected to

<https://chromium.googlesource.com/chromium/src/+log/b92cf6e2a7fd37968ef74f9da653c8bd777b0857..09829acab669a60ebb3a7c403a0b442eac451dc2>

The only relevant looking CL in the range is <https://chromium-review.googlesource.com/c/chromium/src/+1882770>

toyoshim: PTAL? I know your change is only a testing config, but there isn't anything else in the bisect range.

This also seems to be low severity, given that it only allows reading file URL to file URL.

Comment 2 by tiebu...@gmail.com on Thu, Nov 21, 2019, 2:20 AM EST

I write an exploit to steal the chromium cache in Windows10.

[Deleted] **poc.html**

[Deleted] **poc.gif**

Comment 3 by toyoshim@chromium.org on Thu, Nov 21, 2019, 4:34 AM EST Project Member

Cc: yhirano@chromium.org kinuko@chromium.org dharani@chromium.org

Labels: FoundIn-79 FoundIn-80

Components: Blink>SecurityFeature>CORS Blink>Loader

This problem seems to happen when OOR-CORS is enabled.

So the bisect result was correct, maybe it uses the testing config rather than server distributed random config to make the bisect reliable?

OOO-CORS is planned to be launched at m79, and I confirmed that the issue is reproducible on current Chrome 79 beta with chrome://flags/#out-of-blink-cors Enabled.

meacer: You said the severity is low, but do you think this is a stable blocker?

Comment 4 by toyoshim@chromium.org on Thu, Nov 21, 2019, 4:40 AM EST Project Member

Just in case, the issue is reproducible even on Chrome 78 stable with OOR-CORS Enabled. But it's disabled by default. IIRC, 0.00006% users manually enable it.

Comment 5 by toyoshim@chromium.org on Thu, Nov 21, 2019, 5:02 AM EST Project Member

getImageData() also returns bitmap data without throwing an exception if OOR-CORS is enabled.

This issue happens only when file:/// is accessed from file:///.

http(s):// accesses from file:/// are correctly tainted.

Comment 6 by toyoshim@chromium.org on Thu, Nov 21, 2019, 6:13 AM EST Project Member

Status: Started (was: Assigned)

Comment 7 by toyoshim@chromium.org on Thu, Nov 21, 2019, 6:42 AM EST Project Member

The fix is almost ready; <https://chromium-review.googlesource.com/c/chromium/src/+1928606>

Does anyone know if I can write a WPT that expects loading via file:// scheme to test this case.

I know LayoutTests can do it, but haven't wrote such tests in WPT.

Comment 8 by kinuko@chromium.org on Thu, Nov 21, 2019, 7:19 AM EST Project Member

I don't recall there was a way to test file:/// in WPT... unless something has been changed recently.

Comment 9 by yhirano@chromium.org on Thu, Nov 21, 2019, 7:31 AM EST Project Member

IIUC it is not specified: <https://fetch.spec.whatwg.org/#scheme-fetch>

Comment 10 by toyoshim@chromium.org on Thu, Nov 21, 2019, 9:44 AM EST Project Member

yep, I also noticed that the spec does not say anything on file://. so, we won't have the test in WPT regardless of possibility to write such tests.

I will write a layout test maybe in web_tests/fast/canvas/. there, we have similar tests for svg, but we need similar ones for gif or png.

Comment 11 by sheriffbot@chromium.org on Thu, Nov 21, 2019, 10:31 AM EST Project Member

Labels: 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 12 by mea...@chromium.org on Mon, Nov 25, 2019, 9:30 PM EST Project Member

> meacer: You said the severity is low, but do you think this is a stable blocker?

I don't think it is, given that it's low severity bug, but then again, we can re-evaluate whether its medium.

Comment 13 by mea...@chromium.org on Mon, Nov 25, 2019, 9:35 PM EST Project Member

Labels: -Security_Impact-Head Security_Impact-Beta M-79

Changing to impact-beta since the plan is to ship the feature in M79.

Comment 14 by yhirano@chromium.org on Thu, Nov 28, 2019, 6:11 AM EST Project Member

Isn't this a severe problem? IIUC this bugs gives an ability to read local file contents to malicious web developers.

Comment 15 by yhirano@chromium.org on Thu, Nov 28, 2019, 6:40 AM EST Project Member

Ah, sorry, I misunderstood #1.

Comment 16 by bugdroid on Wed, Dec 11, 2019, 5:21 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+69901e65bfea41eab02a3c0e947d076920f3494f>

commit 69901e65bfea41eab02a3c0e947d076920f3494f

Author: Takashi Toyoshima <toyoshim@chromium.org>

Date: Wed Dec 11 10:19:30 2019

OOO-CORS: Set FetchResponseType in FileURLLoader

Once OOR-CORS is enabled, Blink does not apply a file scheme specific check for the canvas taint, and FileURLLoader should set the correct FetchResponseType based on the request mode.

Change-Id: Ie0334d97db6e21b9f4e70c8787f3dc2c4ea1f89f

[Bug-1026546](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1928606>

Commit-Queue: Takashi Toyoshima <toyoshim@chromium.org>

Commit-Queue: Yutaka Hirano <yhirano@chromium.org>

Auto-Submit: Takashi Toyoshima <toyoshim@chromium.org>

Reviewed-by: Yutaka Hirano <yhirano@chromium.org>

Cr-Commit-Position: refs/heads/master@{#723762}

[modify] https://crrev.com/69901e65bfea41eab02a3c0e947d076920f3494f/content/browser/loader/cors_file_origin_browsertest.cc

[modify] https://crrev.com/69901e65bfea41eab02a3c0e947d076920f3494f/content/browser/loader/file_url_loader_factory.cc

[modify] https://crrev.com/69901e65bfea41eab02a3c0e947d076920f3494f/content/browser/loader/file_url_loader_factory.h

[add] <https://crrev.com/69901e65bfea41eab02a3c0e947d076920f3494f/content/test/data/loader/image-taint.html>

Comment 17 by [sheriffbot@chromium.org](#) on Wed, Dec 11, 2019, 9:11 AM EST Project Member

Labels: -Security_Impact-Beta Security_Impact-Stable

Comment 18 by [tiebu...@gmail.com](#) on Thu, Dec 12, 2019, 3:25 AM EST

Hi,

Is it a low severity bug because of the small range of influence?

All the IM app don't think the html file is a dangerous file. So it is can easily sent to other through various channels.

If the chrome is the default browser, we can steal any picture in any folder(IM chat log folder/chrome cache...).

So I think it's very easy to use, and it has relatively high level of threat.

Comment 19 by [toyoshim@chromium.org](#) on Thu, Dec 12, 2019, 3:45 AM EST Project Member

Labels: Merge-Request-80

OOR-CORS is not enabled on the stable, and will be incrementally rolled out.

When 100% users get the feature enabled, the next major update for 80 will happen in a few days.

I will merge this fix to m80.

Comment 20 by [sheriffbot@chromium.org](#) on Thu, Dec 12, 2019, 11:21 AM EST Project Member

Status: Fixed (was: Started)

Please mark security bugs as fixed as soon as the fix lands, and before requesting merges. This update is based on the merge- labels applied to this issue. Please reopen if this update was incorrect.

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

Comment 21 by [sheriffbot@chromium.org](#) on Fri, Dec 13, 2019, 3:50 AM EST Project Member

Labels: -Merge-Request-80 Merge-Approved-80 Hotlist-Merge-Approved

Your change meets the bar and is auto-approved for M80. Please go ahead and merge the CL to branch 3987 (refs/branch-heads/3987) manually. Please contact milestone owner if you have questions.

Merge instructions: <https://www.chromium.org/developers/how-tos/drover>

Owners: govind@(Android), Kariahda@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 22 by [sheriffbot@chromium.org](#) on Fri, Dec 13, 2019, 10:38 AM EST Project Member

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

Comment 23 by [gov...@chromium.org](#) on Fri, Dec 13, 2019, 6:39 PM EST Project Member

Please merge your change to M80 branch 3987 ASAP so we can pick it up for next week beta release. Thank you.

Comment 24 by [gov...@chromium.org](#) on Sun, Dec 15, 2019, 3:53 AM EST Project Member

Requesting to merge to M80 branch 3987 ASAP. Please use branch CQ for merge. Thank you.

Comment 25 by [natashapabrai@google.com](#) on Mon, Dec 16, 2019, 3:08 PM EST Project Member

Labels: reward-topanel

Comment 26 by [gov...@chromium.org](#) on Mon, Dec 16, 2019, 3:25 PM EST Project Member

Requesting to merge to M80 branch 3987 ASAP. Please use branch CQ for merge. Thank you.

Note: We're cutting M80 Beta RC soon for release this week.

Comment 27 by [srinivassista@google.com](#) on Mon, Dec 16, 2019, 6:11 PM EST Project Member

Please get your merges complete to M80 branch asap. I am cutting beta/dev RC today by 5:00 PM PST so would like to include these merges in build before holidays

Comment 28 by [toyoshim@chromium.org](#) on Mon, Dec 16, 2019, 11:50 PM EST Project Member

now it's in CQ: <https://chromium-review.googlesource.com/c/chromium/src/+1971172>

thanks!

Comment 29 by [bugdroid](#) on Tue, Dec 17, 2019, 1:19 AM EST Project Member

Labels: -merge-approved-80 merge-merged-3987 merge-merged-80

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+1887220f4d4e777dc40904d97880c3eea41564ecb>

commit 887220f4d4e777dc40904d97880c3eea41564ecb

Author: Takashi Toyoshima <toyoshim@chromium.org>

Date: Tue Dec 17 06:17:34 2019

OOR-CORS: Set FetchResponseType in FileURLLoader

Once OOR-CORS is enabled, Blink does not apply a file scheme specific check for the canvas taint, and FileURLLoader should set the correct FetchResponseType based on the request mode.

(cherry picked from commit 69901e65bfea41eab02a3c0e947d076920f3494f)

Change-Id: Ie0334d97db6e21b9f4e70c8787f3dc2c4ea1f89f

[Bug-1026546](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1928606>

Commit-Queue: Takashi Toyoshima <toyoshim@chromium.org>

Commit-Queue: Yutaka Hirano <yhirano@chromium.org>

Auto-Submit: Takashi Toyoshima <toyoshim@chromium.org>

Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#723762}
TBR: yhirano@chromium.org
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1971172>
Reviewed-by: Takashi Toyoshima <toyoshim@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#196}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/887220f4d4e777dc40904d97880c3eea41564ecb/content/browser/loader/cors_file_origin_browser_test.cc
[modify] https://crrev.com/887220f4d4e777dc40904d97880c3eea41564ecb/content/browser/loader/file_url_loader_factory.cc
[modify] https://crrev.com/887220f4d4e777dc40904d97880c3eea41564ecb/content/browser/loader/file_url_loader_factory.h
[add] <https://crrev.com/887220f4d4e777dc40904d97880c3eea41564ecb/content/test/data/loader/image-taint.html>

Comment 30 by natashapabrai@google.com on Thu, Dec 19, 2019, 12:34 PM EST Project Member

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-vp@chromium.org with any questions.

Comment 31 by natashapabrai@google.com on Thu, Dec 19, 2019, 12:41 PM EST Project Member

Congrats! The Panel decided to reward \$1,000 for this report!

Comment 32 by natashapabrai@google.com on Thu, Dec 19, 2019, 12:46 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 33 by [bugdroid](#) on Tue, Dec 24, 2019, 4:28 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+e93b5dc01f1fcc6ef4efd0880a8cf60abdd23a42>

commit [e93b5dc01f1fcc6ef4efd0880a8cf60abdd23a42](#)

Author: Yutaka Hirano <yhirano@chromium.org>

Date: Tue Dec 24 09:28:16 2019

Use FetchType::kBASIC in content::CreateFileURLLoader

The header comment is saying "this does not restrict filesystem access

"in any way", so bypassing CORS is the expected behavior.

Bug: 1035575, [4026603](#), [4026546](#)

Change-Id: I1af6a25c9865d8c1f5f367db2f277a9f5c101ac

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1980649>

Reviewed-by: Takashi Toyoshima <toyoshim@chromium.org>

Reviewed-by: Matt Falkenhagen <falken@chromium.org>

Commit-Queue: Yutaka Hirano <yhirano@chromium.org>

Auto-Submit: Yutaka Hirano <yhirano@chromium.org>

Cr-Commit-Position: refs/heads/master@{#727362}

[modify] https://crrev.com/e93b5dc01f1fcc6ef4efd0880a8cf60abdd23a42/content/browser/loader/file_url_loader_factory.cc

Comment 34 by [bugdroid](#) on Fri, Jan 3, 2020, 8:57 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+30e09ff259a285fe072222d3c4417ab70f66d0f>

commit [30e09ff259a285fe072222d3c4417ab70f66d0f](#)

Author: Yutaka Hirano <yhirano@chromium.org>

Date: Sat Jan 04 01:55:27 2020

Use FetchType::kBASIC in content::CreateFileURLLoader

The header comment is saying "this does not restrict filesystem access

"in any way", so bypassing CORS is the expected behavior.

(cherry picked from commit [e93b5dc01f1fcc6ef4efd0880a8cf60abdd23a42](#))

Bug: 1035575, [4026603](#), [4026546](#)

Change-Id: I1af6a25c9865d8c1f5f367db2f277a9f5c101ac

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1980649>

Reviewed-by: Takashi Toyoshima <toyoshim@chromium.org>

Reviewed-by: Matt Falkenhagen <falken@chromium.org>

Commit-Queue: Yutaka Hirano <yhirano@chromium.org>

Auto-Submit: Yutaka Hirano <yhirano@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#727362}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1985834>

Reviewed-by: Shik Chen <shik@chromium.org>

Reviewed-by: Charlie Harrison <charrison@chromium.org>

Commit-Queue: Shik Chen <shik@chromium.org>

Cr-Commit-Position: refs/branch-heads/3987@{#404}

Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/30e09ff259a285fe072222d3c4417ab70f66d0f/content/browser/loader/file_url_loader_factory.cc

Comment 35 by [bugdroid](#) on Tue, Jan 7, 2020, 1:27 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+df83dca40fb3006fddb4a81574b2b3f9fae988b1>

commit [df83dca40fb3006fddb4a81574b2b3f9fae988b1](#)

Author: Yutaka Hirano <yhirano@chromium.org>

Date: Tue Jan 07 06:24:55 2020

Add "BypassSecurityChecks" suffix to content::CreateFileURLLoader

According to the comment "this does not restrict filesystem access

"in any way", so make it look dangerous.

Bug: 1035575, [4026603, 4026546](#)
Change-Id: Iadd64b3b1be417b469b8d85144de21c86f67ceba
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1981414>
Reviewed-by: Matt Falkenhagen <falken@chromium.org>
Reviewed-by: Takashi Toyoshima <toyoshim@chromium.org>
Reviewed-by: Ken Rockot <rockot@google.com>
Commit-Queue: Yutaka Hirano <yhirano@chromium.org>
Cr-Commit-Position: refs/heads/master@{#728817}

[modify] https://crrev.com/d83dca40fb3006fddb4a81574b2b3f9fae988b1/chrome/browser/chrome_content_browser_client.cc
[modify] https://crrev.com/d83dca40fb3006fddb4a81574b2b3f9fae988b1/content/browser/loader/file_url_loader_factory.cc
[modify] https://crrev.com/d83dca40fb3006fddb4a81574b2b3f9fae988b1/content/public/browser/file_url_loader.h
[modify] https://crrev.com/d83dca40fb3006fddb4a81574b2b3f9fae988b1/extensions/browser/extension_protocols.cc

[Comment 36](#) by [bugdroid](#) on Wed, Jan 8, 2020, 12:10 AM EST Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+5a6058700ef20b5fc8b4e69b7684af0b0bc07128>

commit [5a6058700ef20b5fc8b4e69b7684af0b0bc07128](#)
Author: Yutaka Hirano <yhirano@chromium.org>
Date: Wed Jan 08 05:09:07 2020

Add a test for response type for extension resources

This is a regression test for <https://crrev.com/c/1980649>. Resources contained in an extension should be accessible from the extension's background page.

Bug: 1035575, [4026603, 4026546](#)
Change-Id: Ic08cec5d526cc5594a6bf507deca43c96d6258f2
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1981419>
Commit-Queue: Yutaka Hirano <yhirano@chromium.org>
Reviewed-by: Takashi Toyoshima <toyoshim@chromium.org>
Reviewed-by: Karan Bhatia <karandeepb@chromium.org>
Cr-Commit-Position: refs/heads/master@{#729233}

[modify] https://crrev.com/5a6058700ef20b5fc8b4e69b7684af0b0bc07128/chrome/browser/extensions/fetch_apitest.cc

[Comment 37](#) by adetaylor@google.com on Sat, Feb 1, 2020, 8:13 PM EST Project Member

Labels: Release-0-M80

[Comment 38](#) by adetaylor@chromium.org on Mon, Feb 3, 2020, 6:48 PM EST Project Member

Labels: CVE-2020-6408 CVE_description-missing

[Comment 39](#) by adetaylor@chromium.org on Mon, Feb 10, 2020, 4:37 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 40](#) by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST Project Member

Cc: achuith@chromium.org

[Comment 41](#) by [sheriffbot](#) on Thu, Mar 19, 2020, 1:54 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