



☆ Starred by 3 users

**Owner:** antoniosartori@chromium.org

**CC:**  mkwst@chromium.org  
clamy@chromium.org  
 pmeuleman@chromium.org  
arthu...@chromium.org  
antoniosartori@chromium.org

**Status:** Fixed (Closed)

**Components:** [Blink>SecurityFeature>ContentSecurityPolicy](#)

**Modified:** Jun 14, 2021

**Backlog-Rank:** ----

**Editors:** ----

**EstimatedDays:** ----

**NextAction:** ----

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

**Pri:** 1

**Type:** [Bug-Security](#)

Hotlist-Merge-Review  
reward-5000  
Security\_Impact-Stable  
Security\_Severity-Medium  
allpublic  
reward-inprocess  
CVE\_description-submitted  
M-89  
Target-88  
Target-85  
Target-86  
Target-87  
Target-89  
Merge-Rejected-89  
Merge-Rejected-90  
LTS-Security-86  
LTS-Security-Failed-86  
external\_security\_report  
LTS-Security-90  
LTS-Security-Failed-90  
Release-0-M91  
CVE-2021-30532

**BlockedOn:** [issue-1120687](#)  
[View details](#)

**Issue 1117687: Security: Full CSP bypass through filesystem URIs**  
Reported by [gink...@gmail.com](#) on Tue, Aug 18, 2020, 6:08 PM EDT

🔗 Code

#### VULNERABILITY DETAILS

Chrome does not properly inherit a CSP through filesystem URIs even though they share the same origin as the context that creates them.

As long as an attacker can execute JavaScript and load iframes in a victim page, this allows CSP to be fully bypassed by creating a filesystem URI and assigning it to the location of a grandchild frame whose parent is in a different origin than the top frame.

Note that this vulnerability is somewhat similar to [issue-1115628](#). However, I felt that this is worth reporting separately because of the entirely different filesystem scheme and additional restrictions placed on filesystem URIs, requiring a very different frame structure.

#### VERSION

Chrome Version: 84.0.4147.125 stable  
Operating System: Windows 10 OS Version 1903 (Build 18362.959)

This vulnerability is also present in Chrome canary 86.0.4237.0.

#### REPRODUCTION CASE

There are two origins involved in this PoC.  
Attacker origin: <https://8a53k1sq15elsz52-attacker.okay.blue>  
Victim origin: <https://8a53k1sq15elsz52-victim.netlify.app>

All paths on the victim origin have a CSP of: default-src 'none'; script-src 'unsafe-inline'; frame-src <https://8a53k1sq15elsz52-attacker.okay.blue>

There is also a secret value located at <https://8a53k1sq15elsz52-victim.netlify.app/secret>. Because of CSP, pages on the victim origin are normally not able to fetch() the secret.

Therefore, if you visit <https://8a53k1sq15elsz52-victim.netlify.app/secret> an error should appear in the console.

However, if you visit <https://8a53k1sq15elsz52-victim.netlify.app/>, the secret value should appear in an alert().

#### Analysis:

- \* The victim page first loads the attacker page in an iframe.
- \* Upon load of the attacker iframe, the victim page creates a filesystem URI containing HTML which fetches /secret.
- \* The victim page then assigns the filesystem URI to an empty iframe in the attacker page using contentWindow.frames[0].location.
- \* The contents of /secret are then fetch()ed and displayed in an alert(). They could also easily be sent to the attacker's server.

The victim page, the attacker page, the secret page, and the blocked page are attached.

#### CREDIT INFORMATION

Reporter credit: Philip Papurt

**victim.html**  
663 bytes [View](#) [Download](#)

**attacker.html**

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

**secret.html**

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

**blocked.html**

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

[Comment 1](#) by [mpdenton@chromium.org](#) on Wed, Aug 19, 2020, 8:01 PM EDT [Project Member](#)

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

**Owner:** arthu...@chromium.org

**Cc:** mkwst@chromium.org clamy@chromium.org

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

**Components:** Blink>SecurityFeature>ContentSecurityPolicy

Thanks for the report, adding the same owner/CC as ~~issue-4445628~~.

[Comment 2](#) by [sheriffbot](#) on Fri, Aug 21, 2020, 2:14 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 Fri, Aug 21, 2020, 2:50 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 [arthu...@chromium.org](#) on Wed, Sep 2, 2020, 6:21 AM EDT [Project Member](#)

**Cc:** pmeuleman@chromium.org

pmeuleman@ and antoniosartori@ are going to improve how a given policy, like CSP, are inherited across documents/navigations. (PolicyContainer)

There are many CSP bugs around inheritance below:

- [bug-4447687](#)

- [bug-4445628](#)

- [bug-4445208](#)

- [bug-4445045](#)

- [bug-4400467](#)

- [bug-674234](#)

- [bug-657606](#)

I believe their future work might fix several issues in this list.

[Comment 5](#) by [sheriffbot](#) on Wed, Sep 16, 2020, 1:37 PM EDT [Project Member](#)

arthursonzogni: 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 6](#) by [sheriffbot](#) on Wed, Sep 30, 2020, 1:37 PM EDT [Project Member](#)

arthursonzogni: 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 7](#) by [sheriffbot](#) on Wed, Oct 7, 2020, 1:36 PM EDT [Project Member](#)

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

[Comment 8](#) by [sheriffbot](#) on Fri, Oct 30, 2020, 6:46 PM EDT [Project Member](#)

**Labels:** reward-potential

[Comment 9](#) by [sheriffbot](#) on Wed, Nov 18, 2020, 12:22 PM EST [Project Member](#)

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

[Comment 10](#) by [sheriffbot](#) on Wed, Jan 20, 2021, 12:22 PM EST [Project Member](#)

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

[Comment 11](#) by [adetaylor@google.com](#) on Wed, Jan 20, 2021, 6:56 PM EST [Project Member](#)

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

[Comment 12](#) by [sheriffbot](#) on Mon, Feb 22, 2021, 11:16 AM EST [Project Member](#)

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 [arthu...@chromium.org](#) on Tue, Feb 23, 2021, 5:16 AM EST [Project Member](#)

**Labels:** Pri-2

**Blockedon:** 1130587

This would require PolicyContainer to be implemented, with support for CSP, with support for filesystem URL. The way to go is still long.

[Comment 14](#) by [sheriffbot](#) on Tue, Feb 23, 2021, 1:38 PM EST Project Member

**Labels:** -Pri-2 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 15](#) by [nasko@chromium.org](#) on Wed, Feb 24, 2021, 2:12 PM EST Project Member

[security bug triage]: Hey Arthur, can we please prioritize this bug and have it fixed soon? It has been open for a while now. I think recently there has been some work on CSP inheritance and if that's correct, it will be great to get this bug and [issue 4445625](#) fixed.

[Comment 16](#) by [antoniosartori@chromium.org](#) on Thu, Feb 25, 2021, 2:33 AM EST Project Member

This CL <https://chromium-review.googlesource.com/c/chromium/src/+2667858> fixes the inheritance mechanism for CSPs and will close this bug.

[Comment 17](#) by [antoniosartori@chromium.org](#) on Thu, Feb 25, 2021, 2:33 AM EST Project Member

**Status:** Started (was: Assigned)

**Owner:** antoniosartori@chromium.org

[Comment 18](#) by [sheriffbot](#) on Wed, Mar 3, 2021, 12:22 PM EST Project Member

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

[Comment 19](#) by [antoniosartori@chromium.org](#) on Thu, Mar 4, 2021, 11:15 AM EST Project Member

**Status:** Fixed (was: Started)

This has been fixed by <https://chromium-review.googlesource.com/c/chromium/src/+2667858>

Regression test here <https://chromium-review.googlesource.com/c/chromium/src/+2726511>

[Comment 20](#) by [sheriffbot](#) on Thu, Mar 4, 2021, 12:40 PM EST Project Member

**Labels:** reward-topanel

[Comment 21](#) by [sheriffbot](#) on Thu, Mar 4, 2021, 1:54 PM EST Project Member

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

[Comment 22](#) by [sheriffbot](#) on Thu, Mar 4, 2021, 2:20 PM EST Project Member

**Labels:** Merge-Request-89

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M89. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

[Comment 23](#) by [sheriffbot](#) on Thu, Mar 4, 2021, 2:21 PM EST Project Member

**Labels:** -Merge-Request-89 Merge-Review-89 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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:

8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: <http://go/cros-engprodcomponents>

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 24](#) by [Git Watcher](#) on Wed, Mar 10, 2021, 4:25 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+4357dc9e1c28b3225a52925b69ee642937fb110b>

commit [4357dc9e1c28b3225a52925b69ee642937fb110b](#)

Author: Antonio Sartori <[antoniosartori@chromium.org](mailto:antoniosartori@chromium.org)>

Date: Wed Mar 10 09:24:07 2021

CSP: Add internal WPTs for filesystem URL inheritance

This change adds internal Web Platform Tests to check that we correctly inherit Content Security Policies to filesystem URLs.

[Bug-4447687,4449272](#)

Change-Id: I4f78d2dae42ba29d67918764198c71b5def2a5d7

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2726511>

Reviewed-by: Mike West <[mkwst@chromium.org](mailto:mkwst@chromium.org)>

Commit-Queue: Antonio Sartori <[antoniosartori@chromium.org](mailto:antoniosartori@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#861487}

[add] [https://crrev.com/4357dc9e1c28b3225a52925b69ee642937fb110b/third\\_party/blink/web\\_tests/wpt\\_internal/content-security-policy/inheritance/filesystem-url-inherits-from-initiator.sub.html](https://crrev.com/4357dc9e1c28b3225a52925b69ee642937fb110b/third_party/blink/web_tests/wpt_internal/content-security-policy/inheritance/filesystem-url-inherits-from-initiator.sub.html)

[Comment 25](#) by [adetaylor@google.com](#) on Wed, Mar 10, 2021, 4:32 PM EST Project Member

**Labels:** Merge-Request-90

<https://chromium-review.googlesource.com/c/chromium/src/+2667858> landed after M90 branch point, so adding merge request to 90 as well as 89.

[Comment 26](#) by [adetaylor@google.com](#) on Wed, Mar 10, 2021, 5:37 PM EST Project Member

**Labels:** -Merge-Request-90 -Merge-Review-89 Merge-Approved-90 Merge-Rejected-89

Approving merge to M90, branch 4430.

I'm going to reject merge to M89 as it's medium severity, and anything to do with CSP could conceivably have unforeseen compatibility consequences.

[Comment 27](#) by [amyressler@google.com](#) on Wed, Mar 10, 2021, 6:30 PM EST Project Member  
**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-vrp@chromium.org](mailto:security-vrp@chromium.org) with any questions.  
\*\*\*\*\*

[Comment 28](#) by [amyressler@google.com](#) on Wed, Mar 10, 2021, 6:58 PM EST Project Member  
Congratulations, Philip! The VRP Panel has decided to award you \$5,000 for this report. As I mentioned in the other issue, a member from our finance team will be in touch with you soon to arrange payment. Thanks for your efforts and great work!

[Comment 29](#) by [gov...@chromium.org](#) on Thu, Mar 11, 2021, 12:50 AM EST Project Member  
Please merge your change to M90 branch 4430 ASAP. Thank you.

[Comment 30](#) by [antoniosartori@chromium.org](#) on Thu, Mar 11, 2021, 2:11 AM EST Project Member  
Unfortunately the fix <https://chromium-review.googlesource.com/c/chromium/src/+2667858> build upon some other changes and is not easily cherry-pickable. Moreover, as it completely changes the way we inherit CSPs, it comes with its own risks.

Because of that, I would prefer NOT to merge to M90.

(Same goes for all related bugs fixed by the same change.)

[Comment 31](#) by [amyressler@google.com](#) on Thu, Mar 11, 2021, 12:51 PM EST Project Member  
**Labels:** -reward-unpaid reward-inprocess

[Comment 32](#) by [gov...@chromium.org](#) on Thu, Mar 11, 2021, 3:56 PM EST Project Member  
\*\*\* Bulk Edit \*\*\*

Please merge your change to M90 branch 4430 ASAP. Thank you.

[Comment 33](#) by [gov...@chromium.org](#) on Fri, Mar 12, 2021, 1:57 PM EST Project Member  
\*\*\* Bulk Edit \*\*\*

Please merge your change to M90 branch 4430 ASAP.

If it is merged already, please remove "Merge-Approved-90" label,  
apply "merge-merged-4430" & "merge-merged-90" labels and provide merge CL link in bug.

Thank you.

[Comment 34](#) by [gov...@chromium.org](#) on Mon, Mar 15, 2021, 1:26 PM EDT Project Member  
\*\*\* Bulk Edit \*\*\*

Please merge your change to M90 branch 4430 ASAP.

If it is merged already, please remove "Merge-Approved-90" label,  
apply "merge-merged-4430" & "merge-merged-90" labels and provide merge CL link in bug.

Thank you.

[Comment 35](#) by [srinivassista@google.com](#) on Mon, Mar 15, 2021, 4:04 PM EDT Project Member  
Please merge your CL to M90 branch asap ( before 3pm PST, tuesday March 16, 2021). This will help get the CL's into this weeks beta release on wednesday.

[Comment 36](#) by [antoniosartori@chromium.org](#) on Tue, Mar 16, 2021, 3:23 AM EDT Project Member  
**Labels:** -Merge-Approved-90 Merge-Rejected-90

[Comment 37](#) by [antoniosartori@chromium.org](#) on Tue, Mar 16, 2021, 3:24 AM EDT Project Member  
Same as <https://bugs.chromium.org/p/chromium/issues/detail?id=1115298#c33>, not merging in M90.

[Comment 38](#) by [amyressler@chromium.org](#) on Mon, May 24, 2021, 11:28 AM EDT Project Member  
**Labels:** Release-0-M91

[Comment 39](#) by [amyressler@google.com](#) on Mon, May 24, 2021, 2:18 PM EDT Project Member  
**Labels:** CVE-2021-30532 CVE\_description-missing

[Comment 40](#) by [achuith@chromium.org](#) on Tue, Jun 1, 2021, 1:29 PM EDT Project Member  
**Labels:** LTS-Security-86 LTS-Security-Failed-86

[Comment 41](#) by [amyressler@google.com](#) on Mon, Jun 7, 2021, 3:27 PM EDT Project Member  
**Labels:** -CVE\_description-missing CVE\_description-submitted

[Comment 42](#) by [sheriffbot](#) on Fri, Jun 11, 2021, 1:52 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

[Comment 43](#) by [vsavu@google.com](#) on Mon, Jun 14, 2021, 12:37 PM EDT Project Member  
**Labels:** LTS-Security-90 LTS-Security-Failed-90