



☆ Starred by 3 users

Owner:	antoniosartori@chromium.org
CC:	 mkwst@chromium.org clamy@chromium.org  pmeuleman@chromium.org antoniosartori@chromium.org arthu...@chromium.org
Status:	Fixed (Closed)
Components:	Blink>SecurityFeature>ContentSecurityPolicy
Modified:	Jun 14, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
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-2021-30531

Issue 1115628: Security: Full CSP bypass through blob: URIs

Reported by gink...@gmail.com on Wed, Aug 12, 2020, 2:47 PM EDT

↗ Code

VULNERABILITY DETAILS

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

As long as an attacker can execute JavaScript on a victim page, this allows CSP to be entirely bypassed by creating a blob URI and assigning it to the top frame's location.

Note that this vulnerability is not present in Firefox because it treats blob URIs similarly to about:blank. As far as I can tell, the spec is unclear about this:

<https://w3c.github.io/FileAPI/#originOfBlobURL>.

VERSION

Chrome Version: 84.0.4147.105 stable
Operating System: Windows 10 OS Version 1903 (Build 18362.959)

This vulnerability is also present in Chrome canary 86.0.4231.0.

REPRODUCTION CASE

There are two origins involved in this PoC.

attacker origin: <https://cgpq29r51wfnl2zd-attacker.okay.blue>
victim origin: <https://cgpq29r51wfnl2zd-victim.netlify.app>

All paths on the victim origin have a CSP of: default-src 'none'; script-src 'unsafe-inline'

There is also a secret value located at <https://cgpq29r51wfnl2zd-victim.netlify.app/secret>. Because of CSP, the victim origin is normally not able to fetch() the secret.

Therefore, if you visit <https://cgpq29r51wfnl2zd-victim.netlify.app/blocked> an error should appear in the console.

However, if you visit the attacker page at <https://cgpq29r51wfnl2zd-attacker.okay.blue>, the secret value should appear in an alert().

Analysis:

- * The attacker page first loads the victim page in an iframe.
- * The victim page then uses URL.createObjectURL to create a blob URI containing HTML which fetches /secret.
- * The victim page then assigns the blob URI to parent.location. This replaces the parent attacker page, allowing the contents of the blob URI to execute without any CSP restrictions.
- * Note that sandbox="allow-top-navigation" is used on the attacker page so the victim page can set the top frame's location without any user interaction.
- * The contents of /secret are then displayed in an alert(). They could also easily be sent to the attacker's server.

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

CREDIT INFORMATION

Reporter credit: Philip Papurt

attacker.html
147 bytes [View](#) [Download](#)

victim.html

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

blocked.html

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

secret.html

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

[Comment 1](#) by [vakh@chromium.org](#) on Wed, Aug 12, 2020, 6:28 PM EDT [Project Member](#)

Status: Assigned (was: Unconfirmed)

Owner: [mkwst@chromium.org](#)

Cc: [arthu...@chromium.org](#) [clamy@chromium.org](#) [antoniosartori@chromium.org](#)

Components: Blink>SecurityFeature>ContentSecurityPolicy

mkwst: This seems eerily similar to [issue-4445206](#) so assigning it to you.

[Comment 2](#) by [mkwst@chromium.org](#) on Thu, Aug 13, 2020, 3:32 AM EDT [Project Member](#)

Owner: [arthu...@chromium.org](#)

Cc: [-arthu...@chromium.org](#) [mkwst@chromium.org](#)

And I'm assigning it to Arthur. :)

Ideally, it won't reproduce in Canary, as he's made some recent changes in response to other issues.

[Comment 3](#) by [arthursonzogni@google.com](#) on Thu, Aug 13, 2020, 3:56 AM EDT [Project Member](#)

This also reproduce on Canary.

I think I imagine what happens here. This will likely be fixed together with:

- [issue-4400467](#)

- [issue-4445206](#)

which have likely the same cause.

[Comment 4](#) by [vakh@chromium.org](#) on Thu, Aug 13, 2020, 7:26 PM EDT [Project Member](#)

Labels: Security_Severity-Medium Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows

[Comment 5](#) by [sheriffbot](#) on Fri, Aug 14, 2020, 2:13 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 6](#) by [sheriffbot](#) on Fri, Aug 14, 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 7](#) by [sheriffbot](#) on Fri, Aug 28, 2020, 1:37 PM EDT [Project Member](#)

arthursonzogni: 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 8](#) by [arthu...@chromium.org](#) on Wed, Sep 2, 2020, 6:22 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-4445638](#)

- [bug-4446208](#)

- [bug-4446046](#)

- [bug-4400467](#)

- [bug-674234](#)

- [bug-657686](#)

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

[Comment 9](#) 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 10](#) by [sheriffbot](#) on Wed, Oct 7, 2020, 1:37 PM EDT [Project Member](#)

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

[Comment 11](#) by [sheriffbot](#) on Fri, Oct 30, 2020, 6:46 PM EDT [Project Member](#)

Labels: reward-potential

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

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

[Comment 13](#) by [sheriffbot](#) on Wed, Jan 20, 2021, 12:22 PM EST [Project Member](#)

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

Comment 14 by [adetaylor@google.com](#) on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 15 by [nasko@chromium.org](#) on Wed, Feb 24, 2021, 2:13 PM EST Project Member

[security bug triage]: Ping on getting this prioritized along with ~~issue-4447687~~.

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

Status: Started (was: Assigned)

Owner: antoniosartori@chromium.org

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

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

Comment 18 by [antoniosartori@chromium.org](#) on Thu, Mar 4, 2021, 11:14 AM EST Project Member

Status: Fixed (was: Started)

<https://chromium-review.googlesource.com/c/chromium/src/+2725520> has been merged and this is fixed.

Regression test here <https://chromium-review.googlesource.com/c/chromium/src/+2721995>.

Comment 19 by [sheriffbot](#) on Thu, Mar 4, 2021, 12:40 PM EST Project Member

Labels: reward-topanel

Comment 20 by [sheriffbot](#) on Thu, Mar 4, 2021, 1:54 PM EST Project Member

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

Comment 21 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 22 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
- 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 23 by [Git Watcher](#) on Fri, Mar 5, 2021, 5:36 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+89859c05f4f266a60fabcc9f57d8eee20e7ffe61>

commit 89859c05f4f266a60fabcc9f57d8eee20e7ffe61

Author: Antonio Sartori <antoniosartori@chromium.org>

Date: Fri Mar 05 10:35:50 2021

CSP: Add WPTs for inheritance to blob URLs

This CL adds Web Platform Tests checking that we correctly inherit

Content Security Policy from the navigation initiator if a

cross-origin child frame navigates the top frame to a blob URL.

~~Bug-4445638, 4449272~~

Change-Id: I3214333f61eb48542b0ba6712cfb58ee0342f796

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2721995>

Reviewed-by: Mike West <mkwst@chromium.org>

Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>

Commit-Queue: Antonio Sartori <antoniosartori@chromium.org>

Cr-Commit-Position: refs/heads/master@{#860177}

[add] https://crrev.com/89859c05f4f266a60fabcc9f57d8eee20e7ffe61/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/blob-uri-inherits-from-initiator.sub.html

[add] https://crrev.com/89859c05f4f266a60fabcc9f57d8eee20e7ffe61/third_party/blink/web_tests/external/wpt/content-security-policy/inheritance/support/navigate-parent-to-blob.html

Comment 24 by [adetaylor@google.com](#) on Wed, Mar 10, 2021, 4:33 PM EST Project Member

Labels: Merge-Request-90

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

Comment 25 by [adetaylor@google.com](#) on Wed, Mar 10, 2021, 5:38 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 26](#) 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 with any questions.

[Comment 27](#) by amyressler@google.com on Wed, Mar 10, 2021, 6:54 PM EST Project Member

Congratulations, Philip! The VRP Panel has decided to award you \$5000 for this report. Someone from the finance team will be in touch with you soon to arrange payment. Thanks for your contributions and nice work!

[Comment 28](#) by amyressler@google.com on Thu, Mar 11, 2021, 12:51 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 29](#) by antoniosartori@chromium.org on Thu, Mar 11, 2021, 2:35 PM EST Project Member

In [comment#18](#) I copied the wrong CL.

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

[Comment 30](#) by srinivassista@google.com on Mon, Mar 15, 2021, 4:03 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 31](#) by antoniosartori@chromium.org on Tue, Mar 16, 2021, 3:22 AM EDT Project Member

Labels: Merge-Rejected-90

[Comment 32](#) by antoniosartori@chromium.org on Tue, Mar 16, 2021, 3:22 AM EDT Project Member

Labels: -Merge-Approved-90

[Comment 33](#) by antoniosartori@chromium.org on Tue, Mar 16, 2021, 3:23 AM EDT Project Member

Same as <https://bugs.chromium.org/p/chromium/issues/detail?id=1115298#c33>, not merging in M90.

[Comment 34](#) 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 35](#) by gink...@gmail.com on Sat, Apr 17, 2021, 4:29 AM EDT

Would it be possible to change the reporter credit to "Philip Papurt (@ginkoid)" on this issue, [issue-1117687](#), and issue 1190608. Thanks!

[Comment 36](#) by amyressler@chromium.org on Mon, May 24, 2021, 11:29 AM EDT Project Member

Labels: Release-0-M91

[Comment 37](#) by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT Project Member

Labels: CVE-2021-30531 CVE_description-missing

[Comment 38](#) by achuith@chromium.org on Tue, Jun 1, 2021, 1:29 PM EDT Project Member

Labels: LTS-Security-86 LTS-Security-Failed-86

[Comment 39](#) by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 40](#) 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 41](#) by vsavu@google.com on Mon, Jun 14, 2021, 12:39 PM EDT Project Member

Labels: LTS-Security-90 LTS-Security-Failed-90