


[chromium](#) ▾[New issue](#)[Open issues](#) ▾[Search chromium issue](#) ▾[Sign in](#)

★ Starred by 5 users

Owner:wanderview@chromium.org**CC:**

mkwst@chromium.org
wanderview@chromium.org
miketaylr@chromium.org
bcl@chromium.org
est...@chromium.org
bingler@chromium.org
morlovich@chromium.org
 aarontag@chromium.org
mmenke@chromium.org
annev...@gmail.com
holeg...@gmail.com
sporeba@google.com
stefanoduo@google.com

Status:Fixed (*Closed*)**Components:**

[Internals>Network>Cookies](#)
[Blink>ServiceWorker](#)

Modified:

Jul 29, 2022

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

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

2

Type:[Bug-Security](#)

[Security_Severity-Low](#)
[Security_Impact-Stable](#)
[allpublic](#)
[reward-inprocess](#)
[CVE_description-submitted](#)
[external_security_report](#)
[M-98](#)
[external_security_bug](#)
[Release-0-M97](#)
[CVE-2022-0117](#)
[reward-3200](#)

Issue 1115847: Security: SameSite policy bypassed with Service Worker FetchEvent

Reported by kidi...@gmail.com on Thu, Aug 13, 2020, 2:02 AM EDT

 Code

VULNERABILITY DETAILS

It seems Chrome ignores SameSite policy by sending protected cookies when: a request is intercepted by a service worker FetchEvent, then fired from within its context. As developers willingly opt to implement FetchEvent mainly for caching purposes, this behavior undermines CSRF protection expected from setting up SameSite attribute.

I've set up a simple demo page at <https://prong-glory-novel.glitch.me>. The site responds with Set-Cookie the "None" "Lax" "Strict" cookies, then echos the Cookie header value in each response. Without a service worker registered, "cross-site page with a link back here" works as expected; "Lax" sent only for GET method, "Strict" not sent for neither GET nor POST. Once the worker registered however, the page will always show all three cookie values, indicating SameSite policy is not being enforced.

rfc6265bis 5.2.2.2. states two different scenarios for service workers: 1. Requests which simply pass through a Service Worker, 2. Requests which are initiated by the Service Worker itself. It seems Chrome handles the above case in the latter way, presumably because there is a direct call to fetch() is involved. However, I believe they should be handled in the former way; The worker cannot manipulate the Request object in any way, and all it can do with the object is to hand it over to the network or drop it. In my opinion, it is natural to think the request is actually originated from a top-navigation document, so it should be treated like so.

Cross-reported to Mozilla as Firefox exhibits the same behavior. Safari only sends "None" which I suppose is a different problem in itself.

VERSION

Chrome Version: Version 86.0.4231.0 (Official Build) canary (x86_64)

Operating System: macOS 10.15.6

REPRODUCTION CASE

Visit <https://prong-glory-novel.glitch.me>, or setup a local Express server using the attachment.

CREDIT INFORMATION

Reporter credit: Dongsung Kim (@kid1ng)

prong-glory-novel-2020-08-13_055327.tgz

96.3 KB [Download](#)

[Comment 1](#) by vakh@chromium.org on Thu, Aug 13, 2020, 4:46 AM EDT

Project Member

Status: Assigned (was: Unconfirmed)

Owner: chlily@chromium.org

Labels: OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows

Components: Blink>ServiceWorker Internals>Network>Cookies

chlily@ assigning this bug to you for now after poking in the source code.

If you're not the best person to own this, please help find that person and assign it to them or mark the bug as

"Unconfirmed" so it can be re-triaged appropriately. Thanks.

[Comment 2](#) by vakh@chromium.org on Thu, Aug 20, 2020, 3:19 PM EDT Project Member

Cc: est...@chromium.org mkwst@chromium.org mmenke@chromium.org morlovich@chromium.org

[Comment 3](#) by mmenke@chromium.org on Thu, Aug 20, 2020, 3:28 PM EDT Project Member

Is there a reasonable way to behave here, given that ServiceWorkers are global, and may make requests in the background?

[Comment 4](#) by kidi...@gmail.com on Thu, Aug 20, 2020, 10:46 PM EDT

I have no doubt if the request is created from within the worker in the background: i.e., `fetch(new Request(...))`, it should behave as-is. But it seems the disparity arises when, SameSite policy considers where each request is "originated" from, while the behavior in question only considers where one is "initiated" from: i.e., `fetch(request)`.

FetchEvent is partially positioned as a network proxy in this case, often caching responses just like one. So it'd make sense if it'd behave like one transparently, and the current behavior in a sense "modifies" the original request. (Even though the internal logic probably does not work that way.)

This does imply some amendments to rfc6265bis 5.2.2.2. might be in order.

[Comment 5](#) by mmenke@chromium.org on Fri, Aug 21, 2020, 12:30 AM EDT Project Member

Oh, sorry, I misread this as referrer policy. SameSite policy, we're going to need to do something about this more generally to deal with cross-site tracking, so probably not worth worrying about it until that's figured out, except perhaps strict vs lax.

[Comment 6](#) by chlily@chromium.org on Fri, Aug 21, 2020, 1:28 PM EDT Project Member

Owner: morlovich@chromium.org

Labels: Security_Severity-Low Security_Impact-Stable Pri-2

[Comment 7](#) by morlovich@chromium.org on Tue, Aug 25, 2020, 11:15 AM EDT Project Member

Cc: aarontag@chromium.org

FYI Aaron who is checking client hints code for service worker stuff and may find some value in the testcase.

[Comment 8](#) by morlovich@chromium.org on Wed, Aug 26, 2020, 1:58 PM EDT Project Member

Would you say any `fetch()` taking a Request should behave like that?

[Comment 9](#) by morlovich@chromium.org on Wed, Aug 26, 2020, 2:08 PM EDT Project Member

... with Request from a FetchEvent capturing SameSite'ness?

... `fetch` sure has a lot of its own types :(

[Comment 10](#) by kidi...@gmail.com on Wed, Aug 26, 2020, 10:10 PM EDT

I think so, but since I've got no knowledge on the inner workings I can only have a rough idea that internal-Requests should be tagged with SameSite-related attributes.

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

Labels: reward-potential

[Comment 12](#) by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 13 by [sheriffbot](#) on Wed, Mar 10, 2021, 8:04 PM EST Project Member

Labels: reward-potential

Comment 14 by [zhangtiff@google.com](#) on Wed, Mar 17, 2021, 7:12 PM EDT Project Member

Labels: -reward-potential external_security_bug

Comment 15 by [kidi...@gmail.com](#) on Tue, Apr 6, 2021, 8:09 PM EDT

A gentle ping asking how things are moving on this issue. ;)

Comment 16 by [dominickn@chromium.org](#) on Mon, Sep 6, 2021, 8:49 PM EDT Project Member

~~Issue 1246964~~ has been merged into this issue.

Comment 17 by [davidben@chromium.org](#) on Tue, Sep 7, 2021, 10:48 AM EDT Project Member

Cc: [wanderview@chromium.org](#)

Comment 18 by [wanderview@chromium.org](#) on Tue, Sep 7, 2021, 12:27 PM EDT Project Member

I presume this will be fixed when we partition service workers? Once that is enabled we will begin setting the top-level-origin in the IsolationInfo to the SW's StorageKey's top-level site.

Comment 19 by [lukasza@chromium.org](#) on Tue, Sep 7, 2021, 1:37 PM EDT Project Member

Cc: [holeg...@gmail.com](#)

CC-ing [holegary@](#) who reported the duplicate ~~issue 1246964~~

FWIW, I note that in ~~issue 1241188~~ (also reported by [holegary@](#)) there is a discussion about what origin should be used when 1) a POST navigation to [bar.com](#) is initiated by [foo.com](#) and 2) the fetch event handler of a service worker for [bar.com](#) forwards the navigation request to [fetch\(...\)](#). AFAIU, the conclusion is to treat such navigations as if they were initiated by an opaque origin (e.g. "Origin: null", "Sec-Fetch-Site: cross-site", etc.). Maybe similar approach would help for determining whether to send SameSite cookies?

Comment 20 by [wanderview@chromium.org](#) on Tue, Sep 14, 2021, 9:59 AM EDT Project Member

Cc: [ann...@annevk.nl](#)

Adding fetch spec editor to CC.

Comment 21 by [wanderview@chromium.org](#) on Tue, Sep 14, 2021, 10:45 AM EDT Project Member

Cc: -[ann...@annevk.nl](#) [annev...@gmail.com](#)

Comment 22 by [wanderview@chromium.org](#) on Tue, Sep 21, 2021, 11:28 AM EDT Project Member

Cc: [miketaylr@chromium.org](#)

Comment 23 by [wanderview@chromium.org](#) on Tue, Sep 21, 2021, 12:08 PM EDT Project Member

Cc: [bingler@chromium.org](#)

Comment 24 by [wanderview@chromium.org](#) on Tue, Sep 21, 2021, 12:11 PM EDT Project Member

Cc: [bcl@chromium.org](#)

Comment 25 by wanderview@chromium.org on Wed, Sep 29, 2021, 4:21 PM EDT Project Member

Owner: wanderview@chromium.org

I believe my solution for [bug-1241188](#) will also fix this bug. My WIP CL:

<https://chromium-review.googlesource.com/c/chromium/src/+3115917>

Comment 26 by [Git Watcher](#) on Thu, Oct 28, 2021, 3:20 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+da0a6501cf321579bd46a27ff9fba1bb8ea910bb>

commit [da0a6501cf321579bd46a27ff9fba1bb8ea910bb](#)

Author: Ben Kelly <wanderview@chromium.org>

Date: Thu Oct 28 19:19:49 2021

Fetch: Plumb request initiator through passthrough service workers.

This CL contains essentially two changes:

1. The request initiator origin is plumbed through service workers that do `fetch(evt.request)`. In addition to plumbing, this requires changes to how we validate navigation requests in the CorsURLLoaderFactory.
2. Tracks the original destination of a request passed through a service worker. This is then used in the network service to force SameSite=Lax cookies to treat the request as a main frame navigation where appropriate.

For more detailed information about these changes please see the internal design doc at:

<https://docs.google.com/document/d/1KZscujuV7bCFEnzJW-0DaCPU-l40RJmQKoCcl0umTQ/edit?usp=sharing>

In addition, there is some discussion of these features in the following spec issues:

<https://github.com/whatwg/fetch/issues/1321>

<https://github.com/whatwg/fetch/issues/1327>

The test includes WPT tests that verify navigation headers and SameSite cookies. Note, chrome has a couple expected failures in the SameSite cookie tests because of the "lax-allowing-unsafe" intervention that is currently enabled. See:

https://source.chromium.org/chromium/chromium/src/+main:third_party/blink/web_tests/TestExpectations;l=4635;drc=e8133cbf2469adb99c6610483ab78bcfb8cc4c76

~~Bug-1115847~~, [1241188](#)

Change-Id: I7e236fa20aeabb705aef40fcf8d5c36da6d2798c

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3115917>

Reviewed-by: Matt Menke <mmenke@chromium.org>

Reviewed-by: Mutsaers, Liliana <liliana@chromium.org>

Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Reviewed-by: Nasko Oskov <nasko@chromium.org>
Reviewed-by: Łukasz Anforowicz <lukasza@chromium.org>
Commit-Queue: Ben Kelly <wanderview@chromium.org>
Cr-Commit-Position: refs/heads/main@{#936029}

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/platform/loader/fetch/resource_request.h

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https-expected.txt

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/public/cpp/url_request_mojom_traits.h

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/cors/cors_url_loader_unittest.cc

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/content/common/fetch/fetch_request_type_converters.cc

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/public/cpp/resource_request.h

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/core/fetch/fetch_request_data.h

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/net/url_request/url_request_http_job.cc

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/core/fetch/fetch_manager.cc

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/net/url_request/url_request.cc

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-unregister.html

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/platform/loader/fetch/url_loader/request_conversion.cc

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/public/mojom/fetch/fetch_api_request.mojom

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/public/mojom/url_request.mojom

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/net/url_request/url_request_unittest.cc

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/core/fetch/fetch_request_data.cc

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/form-poster.html

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https.html

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js.headers

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/cors/cors_url_loader_factory.cc

[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/location-setter.html

[modify]

https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/cors/cors_url_loader_factory_unittest.cc

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/net/url_request/url_request.h

[modify] <https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/BUILD.gn>

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/cors/cors_url_loader.cc

[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/cors/cors_url_loader.cc
[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/modules/cache_storage/inspector_cache_storage_agent.cc
[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/renderer/core/fetch/request.cc
[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/url_loader.cc
[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/navigation-headers.https.html
[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/navigation-headers-server.py
[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/services/network/public/cpp/url_request_mojom_traits.cc
[modify] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/content/common/background_fetch/background_fetch_types.cc
[add] https://crrev.com/da0a6501cf321579bd46a27ff9fba1bb8ea910bb/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-register.html

Comment 27 by wanderview@chromium.org on Thu, Oct 28, 2021, 3:56 PM EDT Project Member

Note, this still needs two more CLs to fix redirects and navigations from iframes nested like A>B>A.

Comment 28 by [Git Watcher](#) on Thu, Oct 28, 2021, 6:05 PM EDT Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a>

commit [a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a](#)

Author: Alan Screen <awscreen@chromium.org>

Date: Thu Oct 28 22:04:50 2021

Revert "Fetch: Plumb request initiator through passthrough service workers."

This reverts commit [da0a6501cf321579bd46a27ff9fba1bb8ea910bb](#).

Reason for revert: Failure on many bots with the following error message:

The service worker navigation preload request was cancelled before 'preloadResponse' settled. If you intend to use 'preloadResponse', use waitUntil() or respondWith() to wait for the promise to settle.", source: (0)

Original change's description:

> Fetch: Plumb request initiator through passthrough service workers.

>

> This CL contains essentially two changes:

>

> 1. The request initiator origin is plumbed through service workers

> that do `fetch(evt.request)`. In addition to plumbing, this

> requires changes to how we validate navigation requests in the

> CorsURLLoaderFactory.

> 2. Tracks the original destination of a request passed through a

> service worker. This is then used in the network service to force

> SameSite=Lax cookies to treat the request as a main frame navigation

> where appropriate.

>

> For more detailed information about these changes please see the

> internal design doc at:

> internal design doc at:
>
> <https://docs.google.com/document/d/1KZscujuV7bCFEnzJW-0DaCPU-I40RJmQKoCcI0umTQ/edit?usp=sharing>
>
> In addition, there is some discussion of these features in the following
> spec issues:
>
> <https://github.com/whatwg/fetch/issues/1321>
> <https://github.com/whatwg/fetch/issues/1327>
>
> The test includes WPT tests that verify navigation headers and SameSite
> cookies. Note, chrome has a couple expected failures in the SameSite
> cookie tests because of the "lax-allowing-unsafe" intervention that is
> currently enabled. See:
>
>
> https://source.chromium.org/chromium/chromium/src/+main:third_party/blink/web_tests/TestExpectations;l=4635;drc=e8133cbf2469adb99c6610483ab78bcfb8cc4c76
>
> [Bug: 1115847, 1241188](#)
> Change-Id: I7e236fa20aeabb705aef40cf8d5c36da6d2798c
> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3115917>
> Reviewed-by: Matt Menke <mmenke@chromium.org>
> Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
> Reviewed-by: Nasko Oskov <nasko@chromium.org>
> Reviewed-by: Łukasz Anforowicz <lukasza@chromium.org>
> Commit-Queue: Ben Kelly <wanderview@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#936029}

[Bug: 1115847, 1241188](#)

Change-Id: I3044a6d20de172b4a8ab7e39a9f26191580003fa
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3251692>
Auto-Submit: Alan Screen <awscreen@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Alan Screen <awscreen@chromium.org>
Owners-Override: Alan Screen <awscreen@chromium.org>
Cr-Commit-Position: refs/heads/main@{#936125}

[modify]

https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/platform/loader/fetch/resource_request.h

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https-expected.txt

[modify]

https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/public/cpp/url_request_mojom_traits.h

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/cors/cors_url_loader_unittest.cc

[modify]

https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/content/common/fetch/fetch_request_type_converters.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/public/cpp/resource_request.h

[modify] https://crrev.com/abb01b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/public/cpp/resource_request.n

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/core/fetch/fetch_request_data.h

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/net/url_request/url_request_http_job.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/core/fetch/fetch_manager.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/net/url_request/url_request.cc

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-unregister.html

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/platform/loader/fetch/url_loader/request_conversion.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/public/mojom/fetch/fetch_api_request.mojom

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/net/url_request/url_request_unittest.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/public/mojom/url_request.mojom

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/core/fetch/fetch_request_data.cc

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/form-poster.html

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js.headers

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https.html

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/cors/cors_url_loader_factory.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/cors/cors_url_loader_factory_unittest.cc

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/location-setter.html

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/net/url_request/url_request.h

[modify] <https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/BUILD.gn>

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/modules/cache_storage/inspect_or_cache_storage_agent.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/third_party/blink/renderer/core/fetch/request.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/cors/cors_url_loader.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/url_loader.cc

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/navigation-headers.https.html

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/navigation-headers-server.py

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/services/network/public/cpp/url_request_mojom_traits.cc

[modify] https://crrev.com/a6601b2cf2bb7c0a0ffa3c795a0dbc730ef81d1a/content/common/background_fetch/background_fetch_types.cc

[delete] https://crrev.com/b91ae55530943cc4c51f30f90a63ce77c65808dd/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-register.html

Comment 29 by Git Watcher on Fri, Oct 29, 2021, 5:20 PM EDT

Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+2d916566085e4f09bca93021f2b1650ea6237077>

commit [2d916566085e4f09bca93021f2b1650ea6237077](#)

Author: Ben Kelly <wanderview@chromium.org>

Date: Fri Oct 29 21:19:29 2021

Reland "Fetch: Plumb request initiator through passthrough service workers."

This is a reland of [da0a6501cf321579bd46a27ff9fba1bb8ea910bb](#)

This CL also includes a change to mark the two WPT tests as requiring long timeout durations. On my fast build machine with an opt build they take ~5 seconds each to complete and the default timeout is 10 seconds. On slower bots with debug builds its highly likely that these tests would be marked as timing out. This change gives them a 60 second timeout instead.

Original change's description:

> Fetch: Plumb request initiator through passthrough service workers.

>

> This CL contains essentially two changes:

>

> 1. The request initiator origin is plumbed through service workers

> that do `fetch(evt.request)`. In addition to plumbing, this

> requires changes to how we validate navigation requests in the

> CorsURLLoaderFactory.

> 2. Tracks the original destination of a request passed through a

> service worker. This is then used in the network service to force

> SameSite=Lax cookies to treat the request as a main frame navigation

> where appropriate.

>

> For more detailed information about these changes please see the

> internal design doc at:

>

> <https://docs.google.com/document/d/1KZscujuV7bCFEnzJW-0DaCPU-l40RJmQKoCcI0umTQ/edit?usp=sharing>

>

> In addition, there is some discussion of these features in the following

> spec issues:

>

> <https://github.com/whatwg/fetch/issues/1321>

> <https://github.com/whatwg/fetch/issues/1327>

>

> The test includes WPT tests that verify navigation headers and SameSite

> cookies. Note, chrome has a couple expected failures in the SameSite

> cookie tests because of the "lax-allowing-unsafe" intervention that is

> currently enabled. See:

>

>

https://source.chromium.org/chromium/chromium/src/+main:third_party/blink/web_tests/TestExpectations;l=4635;drc=e8133cbf2469adb99c6610483ab78bcfb8cc4c76

>

> Bug: [1115847,1244188](#)

> Change-Id: [I7e236fa20aeabb705aef40fcf8d5c36da6d2798c](#)

> Reviewed on: <https://chromium-review.googlesource.com/#/chromium/src/+2445047>

> Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+/3115917>
> Reviewed-by: Matt Menke <mmenke@chromium.org>
> Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
> Reviewed-by: Nasko Oskov <nasko@chromium.org>
> Reviewed-by: Łukasz Anforowicz <lukasza@chromium.org>
> Commit-Queue: Ben Kelly <wanderview@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#936029}

~~Bug: 1115847, 1241188~~

Change-Id: Ia26acbdd0d7ce6583d9a44f83ed086708657b8bd

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+/3251368>

Reviewed-by: Matt Menke <mmenke@chromium.org>

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

Reviewed-by: Nasko Oskov <nasko@chromium.org>

Reviewed-by: Łukasz Anforowicz <lukasza@chromium.org>

Auto-Submit: Ben Kelly <wanderview@chromium.org>

Commit-Queue: Ben Kelly <wanderview@chromium.org>

Cr-Commit-Position: refs/heads/main@{#936560}

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/platform/loader/fetch/resource_request.h

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https-expected.txt

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/public/cpp/url_request_mojom_traits.h

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/cors/cors_url_loader_unittest.cc

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/content/common/fetch/fetch_request_type_converters.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/public/cpp/resource_request.h

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/core/fetch/fetch_request_data.h

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/net/url_request/url_request_http_job.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/net/url_request/url_request.cc

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/core/fetch/fetch_manager.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-unregister.html

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/platform/loader/fetch/url_loader/request_conversion.cc

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/public/mojom/fetch/fetch_api_request.mojom

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/net/url_request/url_request_unittest.cc

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/public/mojom/url_request.mojom

[modify]

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/core/fetch/fetch_request_data.h

https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/core/fetch/fetch_request_data.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/form-poster.html

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https.html

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/fetch-rewrite-worker.js.headers

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/cors/cors_url_loader_factory.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/location-setter.html

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/cors/cors_url_loader_factory_unittest.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/net/url_request/url_request.h

[modify] <https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/BUILD.gn>

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/cors/cors_url_loader.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/modules/cache_storage/inspector_cache_storage_agent.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/renderer/core/fetch/request.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/navigation-headers.https.html

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/url_loader.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/navigation-headers-server.py

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/services/network/public/cpp/url_request_mojom_traits.cc

[modify] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/content/common/background_fetch/background_fetch_types.cc

[add] https://crrev.com/2d916566085e4f09bca93021f2b1650ea6237077/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-register.html

Comment 30 by [Git Watcher](#) on Tue, Nov 9, 2021, 10:49 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+579df7b562fd2a85591e44fd314a1710c93e6901>

commit [579df7b562fd2a85591e44fd314a1710c93e6901](#)

Author: Ben Kelly <wanderview@chromium.org>

Date: Tue Nov 09 15:48:30 2021

Fetch: Plumb navigation redirect chain through service workers

Navigation redirection works differently than normal redirection.

Navigation requests are made using "manual" redirect mode which means the redirect is not immediately followed. Instead the redirect location is handed back up to the `NavigationURLLoaderImpl` which then manually follows the redirect. This results in a new request being sent for each step in the redirect chain.

This CL plumbs the redirect chain information from

This CL plumbs the redirect chain information from NavigationURLLoaderImpl down through each request so it can be included with requests proxied by a passthrough service worker.

For more detailed information about these changes please see the internal design doc at:

<https://docs.google.com/document/d/1KZscujuV7bCFEnzJW-0DaCPU-l40RJmQKoCcl0umTQ/edit?usp=sharing>

We have rough consensus to make this change in this spec issue:

<https://github.com/whatwg/fetch/issues/1335>

Note, this CL includes some expected test failures. These are due to the "lax-allowing-unsafe" intervention that is currently enabled. See:

https://source.chromium.org/chromium/chromium/src/+main:third_party/blink/web_tests/TestExpectations;l=4635;drc=e8133cbf2469adb99c6610483ab78bcfb8cc4c76

~~Bug-1115847,1241188~~

Change-Id: I2a2a17639e0bec3222684e0d444d6d98a21402ed

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3213310>

Commit-Queue: Ben Kelly <wanderview@chromium.org>

Reviewed-by: Nasko Oskov <nasko@chromium.org>

Reviewed-by: Matt Menke <mmenke@chromium.org>

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

Cr-Commit-Position: refs/heads/main@{#939851}

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/platform/loader/fetch/resource_request.h

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https-expected.txt

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/public/cpp/url_request_mojom_traits.h

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/cors/cors_url_loader_unittest.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/content/common/fetch/fetch_request_type_converters.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/public/cpp/resource_request.h

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/core/fetch/fetch_request_data.h

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/core/fetch/fetch_manager.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/net/url_request/url_request.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/platform/loader/fetch/url_loader_request_conversion.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/public/mojom/fetch/fetch_api_request.mojom

[modify]

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/public/mojom/url_request.mojom

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/net/url_request/url_request_unittest.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/core/fetch/fetch_request_data.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/form-poster.html

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https.html

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/cors/cors_url_loader_factory.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/location-setter.html

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/cors/cors_url_loader_factory_unittest.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/redirect.py

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/net/url_request/url_request.h

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/core/fetch/request.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/renderer/modules/cache_storage/inspector_cache_storage_agent.cc

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/third_party/blink/web_tests/external/wpt/service-workers/service-worker/navigation-headers.https.html

[modify] https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/url_loader.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/content/browser/loader/navigation_url_loader_impl.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/services/network/public/cpp/url_request_mojom_traits.cc

[modify]

https://crrev.com/579df7b562fd2a85591e44fd314a1710c93e6901/content/common/background_fetch/background_fetch_types.cc

Comment 31 by wanderview@chromium.org on Tue, Nov 9, 2021, 10:51 AM EST

Project Member

One more CL is needed here before this can be marked fixed.

Comment 32 by wanderview@chromium.org on Tue, Nov 16, 2021, 5:10 PM EST

Project Member

I have WPT tests demonstrating the remaining problem in this WIP CL:

<https://chromium-review.googlesource.com/c/chromium/src/+3277058>

I'll work on adding the fix now.

Comment 33 by wanderview@chromium.org on Fri, Nov 19, 2021, 4:57 PM EST

Project Member

After working on the tests some more I have come to the conclusion we don't need any more code changes in this bug. There are still some places where we incorrectly send SameSite cookies from service workers, but those require storage partitioning to fix. That work is underway and will ship separately.

Keeping this open until I get review and confirmation of my understanding in the tests.

Comment 34 by [Git Watcher](#) on Mon, Nov 22, 2021, 6:27 PM EST

Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+53f29314ad19fc5e0e0500de0d9544b856a45e32>

commit [53f29314ad19fc5e0e0500de0d9544b856a45e32](#)

Author: Ben Kelly <wanderview@chromium.org>

Date: Mon Nov 22 23:26:45 2021

Add WPT tests for SameSite cookies in ServiceWorkers with nested frames.

This CL adds a number of new cases to the service worker SameSite cookies test. The cases break down into two general types:

1. Cases where A1 frames B frames A2, and then A2 calls window.open() to an A origin URL.
2. Cases where A1 frames B frames A2, and then A2 sets the location to an A origin URL.

For (1) we expect SameSite strict cookies to be sent because window.open() creates a top-level context that will have a populated site-for-cookies and the initiator is same-origin (regardless of the cross-site ancestor chain).

For (2) we expect only SameSite=None cookies to be sent. This is because setting the location results in a navigation to an A1->B->A3 nested frame with an empty site-for-cookies.

We currently fail the passthrough and change-request cases for (2). We plan to fix this as part of storage partitioning with an ancestor chain bit in the StorageKey. See:

<https://github.com/privacycg/storage-partitioning/issues/25>

This CL also includes some minor cleanup of the WPT test and associated resources.

[Bug: 1115847](#)

Change-Id: I9002e60a271ae95d1d702068d44b30bd0e33b5dc

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3277058>

Reviewed-by: Steven Binger <binger@chromium.org>

Commit-Queue: Ben Kelly <wanderview@chromium.org>

Cr-Commit-Position: refs/heads/main@{#944293}

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https-expected.txt

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-unregister.html

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/same-site-cookies.https.html

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/location-setter.html

[add] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/window-opener.html

[add] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/nested-parent.html

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies.https-expected.txt

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/form-poster.html

[modify] https://crrev.com/53f29314ad19fc5e0e0500de0d9544b856a45e32/third_party/blink/web_tests/external/wpt/service-workers/service-worker/resources/same-site-cookies-register.html

Comment 35 by [wanderview@chromium.org](#) on Tue, Nov 23, 2021, 9:37 AM EST Project Member

Status: Fixed (was: Assigned)

Labels: M-98

This is fixed in M-98. Due to the size of the CLs I'd prefer not to merge them to earlier branches.

Comment 36 by [sheriffbot](#) on Tue, Nov 23, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 37 by [sheriffbot](#) on Tue, Nov 23, 2021, 1:42 PM EST Project Member

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

Comment 38 by [amyressler@chromium.org](#) on Tue, Jan 4, 2022, 12:35 PM EST Project Member

Labels: Release-0-M97

Comment 39 by [amyressler@google.com](#) on Tue, Jan 4, 2022, 1:35 PM EST Project Member

Labels: CVE-2022-0117 CVE_description-missing

Comment 40 by [sheriffbot](#) on Tue, Mar 1, 2022, 1:30 PM EST 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 [amyressler@google.com](#) on Thu, Mar 10, 2022, 10:40 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-3200

*** 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 42 by [amyressler@chromium.org](#) on Thu, Mar 10, 2022, 11:41 PM EST Project Member

Congratulations, Dongsung! The VRP Panel has decided to award you \$3000 for this report. Thank you for your efforts and nice work. Please accept our apologies in the delay in getting this issue to resolution and through the VRP Panel. We have added a \$200 bonus to your reward due to the significant delay.

added a \$200 bonus to your reward due to the significant delay.

[Comment 43](#) by kidi...@gmail.com on Fri, Mar 11, 2022, 8:47 PM EST

Amazing! Thank you for all the work. Let me know if there's anything I should further follow up on.

[Comment 44](#) by amyressler@chromium.org on Mon, Mar 14, 2022, 4:58 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

I should have mentioned, if you haven't already, someone from our finance team will be in touch soon to begin payments onboarding. Thank you again for your report!

[Comment 45](#) by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)