☆ Starred by 2 users

Owner:	yoavweiss@chromium.org
CC:	mkwst@chromium.org yoavweiss@chromium.org antoniosartori@chromium.org panicker@chromium.org arthu...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>PerformanceAPIs Blink>SecurityFeature>ContentSecurityPolicy
Modified:	Mar 16, 2021
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
allpublic
reward-inprocess
CVE_description-submitted
Release-0-M89
external_security_report
CVE-2021-21183

Issue 1105875: Security: XS-Leak with Resource Timing API and CSP Embedded Enforcement

Reported by takas...@shift-js.info on Wed, Jul 15, 2020, 10:46 AM EDT

Code

VULNERABILITY DETAILS

When we get an error by `csp` attribute of `iframe` tags (i.e. CSP Embedded Enforcement), `name` property of `PerformanceResourceTiming` for the iframe turns into `data:,`.
This may allow attackers to check whether a Cross-Origin response has a more restrictive CSP than one specified in `csp` attribute, or not.
In other words, this behavior of CSPEE and Resource Timing API can be utilized as XS-Leak.

Notably, express, a famous server-side library of Node.js, returns `default-src: 'none'` header with its default error page. For instance, the following HTTP server written in Node.js returns `default-src: 'none'` with 404 when we access `/foobar`, while `/` returns 200 without any CSP header.

~~~
```js
const express = require('express')
const app = express()

app.get('/', (req, res) => res.send('Hello World!'))
app.listen(25252, () => { })
```
~~~

This fact means that, in the case of express, attackers can know whether a cross-origin application by express returns a default error page or not. Here's the PoC:

~~~
```html
<script>
  window.onload = () => {
    performance.getEntriesByType("resource").map((r, i) => {
      if (r.name === "data:,") {
        alert(`record ${i} tells us we got default error page!`);
      } else {
        alert(`record ${i} tells us we got a normal page!`);
      }
    })
  }
</script>
<iframe id="a" src="http://localhost:25252/" csp="default-src 'none'"></iframe>
<iframe id="b" src="http://localhost:25252/404" csp="default-src 'none'"></iframe>
```
~~~

Considering a lot of web apps are using express still now, I believe this XS-Leak vector has an impact to some extent.

VERSION
Chrome Version: Version 83.0.4103.61 (Official Build) (64-bit) + stable
Operating System: Ubuntu 20.04

REPRODUCTION CASE

1. Download attached files (`poc.html` and `index.js`) into a same directory.
2. In the directory in which downloaded files are placed, run `npm install && node index.js`.
3. Open `poc.html`.

CREDIT INFORMATION
Reporter credit: Takashi Yoneuchi (@y0n3uchy)

index.js
139 bytes View Download

index.html
508 bytes View Download

Comment 1 by metzman@chromium.org on Fri, Jul 17, 2020, 2:47 PM EDT Project Member

Status: Available (was: Unconfirmed)
Cc: mkwst@chromium.org
Labels: Security_Severity-Low Security_Impact-Stable OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>SecurityFeature

I beleive I was able to reproduce the intended behavior of the POC.
mkwest@ could you please take a look?

Comment 2 by sheriffbot on Fri, Jul 17, 2020, 2:54 PM EDT Project Member

Labels: -Pri-1 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 3 by mkwst@chromium.org on Mon, Jul 20, 2020, 2:00 AM EDT Project Member

Status: Assigned (was: Available)
Owner: y...@yoav.ws
Cc: yoavweiss@chromium.org
Components: -Blink>SecurityFeature Blink>SecurityFeature>ContentSecurityPolicy Blink>PerformanceAPIs

It seems to me that error pages shouldn't show up in performance timing APIs. Yoav, is this intentional?

Comment 4 by mkwst@chromium.org on Mon, Jul 20, 2020, 2:02 AM EDT Project Member

Cc: antoniosartori@chromium.org

I suspect this might be happening because the navigation to the error page is performed by Blink, rather than blocking the navigation with an error interstitial in the browser, which antoniosartori@ is working through.

Comment 5 by npm@chromium.org on Mon, Jul 20, 2020, 10:53 AM EDT Project Member

We do intentionally expose some error pages in Resource Timing. Perhaps what we need is further restricting what information is exposed in those cases?

Comment 6 by mkwst@chromium.org on Mon, Jul 20, 2020, 11:24 AM EDT Project Member

I'd prefer that we not explicitly distinguish between a cross-origin page that loaded successfully, and one that caused a violation of some sort (XFO, CSP, whatever). Listing the URL that the embedding page already knows is fine, pointing out that it was an error page seems less fine.

Comment 7 by npm@chromium.org on Mon, Jul 20, 2020, 11:55 AM EDT Project Member

Right, and per the spec (https://w3c.github.io/resource-timing/#sec-performanceresourcetiming), for name: "This attribute MUST return the resolved URL of the requested resource. This attribute MUST NOT change even if the fetch redirected to a different URL." so I think this means the name should not be set to 'data:,'. Somehow the original requested URL is being lost.

Comment 8 by yoavweiss@chromium.org on Tue, Jul 28, 2020, 4:51 AM EDT Project Member

Owner: yoavweiss@chromium.org

It seems to me like the correct behavior we want here is:
* iframe URLs are reported using regular Performance Entries - Otherwise, that would also enable to distinguish between an error page and a non-error page
* Those URLs should not change if the iframe loading was terminated by CSP's embedded enforcement

Does that match y'all's understanding?

Comment 9 by npm@chromium.org on Tue, Jul 28, 2020, 11:11 AM EDT Project Member

That makes sense to me. BTW I closed ~~issue 1105834~~ recently as it was fixed in 84, so perhaps double check that this is still an issue.

Comment 10 by sheriffbot on Fri, Oct 30, 2020, 6:46 PM EDT Project Member

Labels: reward-potential

Comment 11 by yoavweiss@chromium.org on Mon, Dec 7, 2020, 6:36 PM EST Project Member

Status: Started (was: Assigned)

I'm able to reproduce the issue to some extent (I see that cross-origin blocked entries are not reported at all, rather than reported as 'data:', but the effect is the same).

Comment 12 by yoavweiss@chromium.org on Tue, Dec 8, 2020, 4:35 AM EST Project Member

https://chromium-review.googlesource.com/c/chromium/src/+/2567925 also solves this issue.

Comment 13 by bugdroid on Tue, Dec 8, 2020, 7:41 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/eb493883a20b1e05a759c3006ee35a93d10ffa72

commit eb493883a20b1e05a759c3006ee35a93d10ffa72
Author: Yoav Weiss <yoavweiss@chromium.org>
Date: Tue Dec 08 12:40:16 2020

[resource-timing] ResourceTimingInfo for failed navigations

Failed navigations currently don't get a ResourceTiming entry.
This CL changes that by properly reporting them.

~~Bug: 1131020~~, ~~1105875~~
Change-Id: I0808f35e1b0d596c2bafa7630ed873c947254c5e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2567925
Commit-Queue: Yoav Weiss <yoavweiss@chromium.org>
Reviewed-by: Arthur Sonzogni <arthursonzogni@chromium.org>
Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Cr-Commit-Position: refs/heads/master@{#834675}

[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/public/web/web_security_policy.h

[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/content/renderer/render_thread_impl.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/core/exported/web_security_policy.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/platform/weborigin/scheme_registry.h
[add] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/web_tests/external/wpt/resource-timing/iframe-failed-commit.html
[add] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/web_tests/external/wpt/resource-timing/resources/csp-default-none.html.headers
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/core/frame/remote_frame_owner.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/core/loader/document_loader.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/content/renderer/render_frame_impl.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/platform/weborigin/scheme_registry.cc
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/public/web/web_navigation_params.h
[modify] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/renderer/core/loader/document_loader.h
[add] https://crrev.com/eb493883a20b1e05a759c3006ee35a93d10ffa72/third_party/blink/web_tests/external/wpt/resource-timing/resources/csp-default-none.html

Comment 14 by yoavweiss@chromium.org on Tue, Dec 8, 2020, 7:51 AM EST Project Member

Status: Fixed (was: Started)

Comment 15 by sheriffbot on Tue, Dec 8, 2020, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 16 by sheriffbot on Tue, Dec 8, 2020, 1:59 PM EST Project Member

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

Comment 17 by adetaylor@google.com on Wed, Dec 16, 2020, 7:08 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-vrp@chromium.org with any questions.
****

Comment 18 by adetaylor@google.com on Wed, Dec 16, 2020, 7:23 PM EST Project Member

Congratulations, the VRP panel has decided to award $1000 for this bug.

Comment 19 by adetaylor@google.com on Thu, Dec 17, 2020, 1:38 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 20 by adetaylor@google.com on Wed, Jan 20, 2021, 6:56 PM EST Project Member

Labels: -reward-potential external_security_report

Comment 21 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 22 by adetaylor@google.com on Mon, Mar 1, 2021, 7:28 PM EST Project Member

Labels: CVE-2021-21183 CVE_description-missing

Comment 23 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 24 by sheriffbot on Tue, Mar 16, 2021, 1:51 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