☆ Starred by 5 users

Owner:	yoavweiss@chromium.org
CC:	falken@chromium.org mkwst@chromium.org yhirano@chromium.org nhiroki@chromium.org lingqi@chromium.org arthu...@chromium.org tommckee@chromium.org toyoshim@chromium.org swarnasree.mukkala@chromium.org nasko@chromium.org panicker@chromium.org yoavweiss@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>PerformanceAPIs Blink>Loader
Modified:	Mar 16, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows, Mac
Pri:	2
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Severity-Low
Security_Impact-Stable
Arch-x86_64
Hotlist-Interop
allpublic
reward-inprocess
Via-Wizard-API
Triaged-ET
CVE_description-submitted
M-87
Target-87
FoundIn-85
FoundIn-86
FoundIn-87

Issue 1131929: [Resource Timing] Missing PerformanceResourceTiming entries for iframe Requests that don't receive a Response

Reported by faste...@gmail.com on Thu, Sep 24, 2020, 11:07 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.53 Safari/537.36

Steps to reproduce the problem:
1. Load test.html
2. Observe that Broken never gets a performance entry

What is the expected behavior?
I expect all cases to generate a performance entry as it does in Firefox and IE (I'm not able to test Safari).

What went wrong?
The broken iframe does not have an entry.

Did this work before? No

Does this work in other browsers? Yes

Chrome version: 86.0.4240.53 Channel: beta
OS Version: 10.0
Flash Version:

This seems related to ~~Issue 460879~~ but specifically for iframes. It doesn't seem like iframes were specifically excluded in https://github.com/w3c/resource-timing/issues/12.

test.html
1.1 KB View Download

Comment 1 by jhansi.muppalla@chromium.org on Thu, Sep 24, 2020, 11:15 PM EDT Project Member

Labels: Needs-Triage-M86

Comment 2 by swarnasree.mukkala@chromium.org on Fri, Sep 25, 2020, 3:50 AM EDT Project Member

Status: Untriaged (was: Unconfirmed)
Cc: swarnasree.mukkala@chromium.org
Labels: Triaged-ET M-87 FoundIn-87 Target-87 FoundIn-86 FoundIn-85 OS-Mac

Able to reproduce the issue on reported chrome #86.0.4240.53 using Windows 10 and Mac 10.15.6 by following steps as per comment #0.
NOTE: Issue is not seen on Ubuntu 16.04

Reproducible in:

Canary: 87.0.4273.0
Dev: 87.0.4270.0
Beta: 86.0.4240.55
stable: 85.0.4183.121

The behavior is seen from M-75. This is non regression issue hence marking it as untriaged and requesting some one from dev team to look into the issue.
Thanks..

Comment 3 by tdres...@chromium.org on Thu, Oct 15, 2020, 3:53 PM EDT Project Member
Status: Assigned (was: Untriaged)
Owner: npm@chromium.org

Over to npm@ for triage.

Comment 4 by npm@chromium.org on Thu, Oct 15, 2020, 5:06 PM EDT Project Member
Components: Blink>HTML>IFrame Blink>Loader

We do need an entry for a failed request, as it is a security problem to enable distinguishing between successful and failed fetches. From what I understand the iframe entries are created from Navigation Timing for the iframe:

DocumentLoader::BodyLoadingFinished
RemoteFrameOwner::AddResourceTiming
RenderFrameHostImpl::ForwardResourceTimingToParent

Obviously we don't need/have a NavigationTiming entry for an iframe that does not end up existing. But I imagine DocumentLoader will still exist for a failed iframe? Is it possible for loader folks to call the AddResourceTiming method on failure as well?

Comment 5 by npm@chromium.org on Thu, Oct 15, 2020, 5:06 PM EDT Project Member
Status: Untriaged (was: Assigned)

Comment 6 by npm@chromium.org on Thu, Oct 15, 2020, 5:07 PM EDT Project Member
Owner: ----

Comment 7 by a_deleted_user on Mon, Oct 19, 2020, 4:45 PM EDT
Components: -Blink>HTML>IFrame

Comment 8 by npm@chromium.org on Thu, Oct 22, 2020, 3:12 PM EDT Project Member
Status: Available (was: Untriaged)

Ok, marking as available for now, look forward to thoughts from Blink Loader folks.

Comment 9 by toyoshim@chromium.org on Thu, Oct 22, 2020, 8:54 PM EDT Project Member
Cc: nhiroki@chromium.org falken@chromium.org toyoshim@chromium.org
Labels: Type-Bug-Security

Comment 10 by toyoshim@chromium.org on Thu, Oct 22, 2020, 9:09 PM EDT Project Member
Cc: lingqi@chromium.org

Comment 11 by ochang@google.com on Mon, Oct 26, 2020, 2:16 AM EDT Project Member
Labels: Security_Severity-Low Security_Impact-Stable

Severity-Low as this gives the ability to distinguish between failed and successful fetches.

Comment 12 by sheriffbot on Fri, Oct 30, 2020, 6:46 PM EDT Project Member
Labels: reward-potential

Comment 13 by yoavweiss@chromium.org on Tue, Dec 1, 2020, 11:54 AM EST Project Member
Status: Assigned (was: Available)
Owner: yoavweiss@chromium.org

The cause for this seems to be:
* The response that DocumentLoader gets for the error iframe is a chrome-error:// scheme, so not reported (we only report HTTP pages)
* Even if we were to report it, the response URL is the error URL, not the original request URL.

I'm taking a stab at fixing this.

Comment 14 by yoavweiss@chromium.org on Thu, Dec 3, 2020, 1:52 AM EST Project Member
Status: Started (was: Assigned)

https://chromium-review.googlesource.com/c/chromium/src/+/2567925 should fix the error case (still missing tests).
Might be interesting to also look at e.g. 204s to see if they are properly reported.

Comment 15 by yoavweiss@chromium.org on Thu, Dec 3, 2020, 3:01 AM EST Project Member
Cc: yhirano@chromium.org

Comment 16 by yoavweiss@chromium.org on Fri, Dec 4, 2020, 3:14 AM EST Project Member
Cc: arthu...@chromium.org

Comment 17 by arthu...@chromium.org on Fri, Dec 4, 2020, 5:13 AM EST Project Member
Cc: nasko@chromium.org

The pending fix is:
https://chromium-review.googlesource.com/c/chromium/src/+/2567925
which make error documents to reveal informations to their parents, the same way normal documents does.

So to fix the cross-origin leak, we need to send more data toward the cross-origin parent? This sounds counter-intuitive at first, and potentially risky, since those are internal pages. We need to double check the cure is not worse than the disease.

I don't know anything about the PerformanceObserver, so I can't help much. What kind of new data will be sent to the parent?
I tried locally, this give something like this:

```
{
  connectEnd: 0
  connectStart: 0
  decodedBodySize: 0
  domainLookupEnd: 0
  domainLookupStart: 0
  duration: 23.164999904111028
  encodedBodySize: 0
  entryType: "resource"
  fetchStart: 13993.94499999471
  initiatorType: "iframe"
  length: 0
  name: "https://example.com/"
  nextHopProtocol: ""
  redirectEnd: 0
  redirectStart: 0
  requestStart: 0
  responseEnd: 14017.109999898821
  responseStart: 0
  secureConnectionStart: 0
  serverTiming: Array(0)
  startTime: 13993.94499999471
  transferSize: 0
  workerStart: 0
}
```

Maybe this will be okay. Could you please double check this won't be a problem?
To be worthwhile doing, the new data should be indistinguishable from non-error pages. Is it the case? Otherwise, we would end up with the original problem.

+CC nasko@ as FYI. Since this is about error pages, and you worked on isolating some of them.

Comment 18 by yoavweiss@chromium.org on Mon, Dec 7, 2020, 12:55 PM EST Project Member

Cc: mkwst@chromium.org

> So to fix the cross-origin leak, we need to send more data toward the cross-origin parent?

Yes. As this information is exposed for iframes, not exposing it for some reveals information about them.

> We need to double check the cure is not worse than the disease.

Makes sense to be sure.

> What kind of new data will be sent to the parent?

We do report non-null startTime, fetchStart, responseEnd and duration, where startTime==fetchStart and duration == (responseEnd - fetchStart)

name is the pre-redirect, pre-error URL

> To be worthwhile doing, the new data should be indistinguishable from non-error pages. Is it the case?

I believe so, other than timing attacks. But the current values I see would make sense also for non-error pages. (i.e. they are not extremely low)

As the CL is now ready to land, let me know if y'all think it's safe to do.

Comment 19 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: 1131929~~, ~~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 20 by yoavweiss@chromium.org on Tue, Dec 8, 2020, 7:51 AM EST Project Member

Status: Fixed (was: Started)

Comment 21 by sheriffbot on Tue, Dec 8, 2020, 12:43 PM EST Project Member

Labels: reward-topanel

Comment 22 by sheriffbot on Tue, Dec 8, 2020, 1:59 PM EST Project Member

Labels: Restrict-View-SecurityNotify

Comment 23 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 24 by adetaylor@google.com on Wed, Dec 16, 2020, 7:25 PM EST Project Member

Congratulations! We deemed this to be a security bug and the VRP bug has deemed it is eligible for a reward of $1000 :) Someone from our finance team will be in touch.
We'll also credit this to you in the Chrome release notes - how would you like to be credited?

Comment 25 by faste...@gmail.com on Wed, Dec 16, 2020, 7:50 PM EST

I appreciate the reward and the credit! My full name is fine for credit purposes, James Hartig.

The target version is 87? Will this bug be updated once it's released?

Comment 26 by yoavweiss@chromium.org on Thu, Dec 17, 2020, 2:40 AM EST Project Member

Labels: Merge-Request-88

Right now it's targeted for 89. I'll attempt to merge back to 88. As Security Severity is low, I don't think this requires a stable re-spin for 87 (but y'all let me know if I'm wrong on that front)

Comment 27 by sheriffbot on Thu, Dec 17, 2020, 2:42 AM EST Project Member

Labels: -Merge-Request-88 Merge-Review-88 Hotlist-Merge-Review

This bug requires manual review: M88's targeted beta branch promotion date has already passed, so this requires manual review
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: govind@(Android), bindusuvarna@(iOS), dgagnon@(ChromeOS), srinivassista @(Desktop)

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

Comment 28 by yoavweiss@chromium.org on Thu, Dec 17, 2020, 2:54 AM EST Project Member

1. We are in phase 2, and this is a low severity non-regression security issue. As such I'm not sure it merits a merge back to 88.
2. https://chromium-review.googlesource.com/c/chromium/src/+/2567925
3. The change has landed in M88. I verified and tested it, but not sure if anyone else did.
4. I don't believe so
5. This is a security issue resulting in cross-site information leaks
6. No
7. N/A

Comment 29 by faste...@gmail.com on Thu, Dec 17, 2020, 7:59 AM EST

> Right now it's targeted for 89. I'll attempt to merge back to 88.

Thanks for the clarification. Makes sense I just misunderstood the labels.

Comment 30 by adetaylor@google.com on Thu, Dec 17, 2020, 1:37 PM EST Project Member

Labels: -Merge-Review-88 Merge-Rejected-88

Hi Yoav & James, I agree with #c28 that this doesn't merit a merge. It'll be released in M89.

Comment 31 by adetaylor@google.com on Thu, Dec 17, 2020, 1:37 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 32 by yoavweiss@chromium.org on Fri, Jan 15, 2021, 12:05 PM EST Project Member

Cc: tommckee@chromium.org

Comment 33 by adetaylor@google.com on Fri, Jan 15, 2021, 1:55 PM EST Project Member

Labels: external_security_report

Comment 34 by adetaylor@google.com on Wed, Jan 20, 2021, 7:01 PM EST Project Member

Labels: -reward-potential

Comment 35 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 36 by adetaylor@google.com on Mon, Mar 1, 2021, 7:28 PM EST Project Member

Labels: CVE-2021-21184 CVE_description-missing

Comment 37 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 38 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