☆ Starred by 4 users

| | |
|---|---|
| **Owner:** | yoavweiss@chromium.org |
| **CC:** | noam....@gmail.com<br>yhirano@chromium.org<br>yoavweiss@chromium.org<br>adetaylor@chromium.org<br>terjanq@google.com<br>npm@chromium.org<br>ahemery@chromium.org<br>altimin@chromium.org<br>dgozman@chromium.org<br>toyoshim@chromium.org<br>sporeba@google.com<br>panicker@chromium.org<br>stefanoduo@google.com |
| **Status:** | Fixed *(Closed)* |
| **Components:** | Internals>Network<br>Blink>PerformanceAPIs>NavigationTiming<br>Blink>PerformanceAPIs>ServerTiming |
| **Modified:** | Jul 29, 2022 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros |
| **Pri:** | 2 |
| **Type:** | Bug-Security |

Reward-1000
Security_Severity-Low
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-96
Security_Impact-Extended
Release-0-M100
CVE-2022-1146

## Issue 1290150: Security: redirect detection via Performance API

Reported by datta...@gmail.com on Sun, Jan 23, 2022, 10:59 AM EST Project Member

Code

**This template is ONLY for reporting security bugs. If you are reporting a Download Protection Bypass bug, please use the "Security - Download Protection" template. For all other reports, please use a different template.**

**Please READ THIS FAQ before filing a bug: https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/faq.md**

**Please see the following link for instructions on filing security bugs: https://www.chromium.org/Home/chromium-security/reporting-security-bugs**

**Reports may be eligible for reward payments under the Chrome VRP: http://g.co/ChromeBugRewards**

**NOTE: Security bugs are normally made public once a fix has been widely deployed.**

**------------------------**

**VULNERABILITY DETAILS**
performance.getEntriesByName(...)[0].duration allows detection of redirects cross-origin.

**VERSION**
Chrome Version: 97.0.4692.99 + stable
Chrome Version: 98.0.4758.66 + beta
Operating System: Manjaro Linux, 5.15 kernel

**REPRODUCTION CASE**
1) Download the attached index.html file.
2) Run a python HTTP server by running `python -m http.server` in the same directory as the index.html file.
3) Open http://localhost:8000/index.html in Chrome
4) Open DevTools Console
5) https://google.com should be correctly identified as a redirect, whereas, https://www.google.com should be identified as a URL without a redirect.

Probable Explanation:
When we are measuring the time using performance.now() across the await fetch() call, we are measuring the total amount of time it has taken for the browser to fetch the page including the time spent retrieving redirects. performance.getEntriesByName(...)[0].duration on the other hand, appears to only report the amount of time taken for the browser to complete the last request. We can use this discrepancy to detect if a URL is a redirect or not.

Security implications:
Identifying whether or not a URL is a redirect could allow websites to fingerprint and detect whether or not a user has an account on a different site. To demonstrate this attack, I've attached a poc.html, which will try to detect if the user is logged into a Gmail account in the current browsing session using this bug (by checking if https://mail.google.com/mail/u/0/ is a redirect or not)

redirect or not).

**CREDIT INFORMATION**
Reporter credit: Sohom Datta

**index.html**
1.3 KB View Download

**poc.html**
1.4 KB View Download

Comment 1 by sheriffbot on Sun, Jan 23, 2022, 11:02 AM EST

**Labels:** external_security_report

Comment 2 Deleted

Comment 3 Deleted

Comment 4 by datta...@gmail.com on Mon, Jan 24, 2022, 3:44 AM EST Project Member

Some notes about stuff I found while doing some more digging around:
- This (redirect detection) seems reproducible even in Android
- The threshold (of the difference) seems to vary a bit from machine, tho based on my availiable hardware, 5ms works for most computers, on Android I had to increase the threshold to 10ms
- We can also use the difference between the first performance.now() call and the performance.getEntriesByName(...)[0].startTime or performance.getEntriesByName(...)[0].fetchStart to check if the url is a redirect.
- Firefox does not appear to have this specific issue since it appears to report the total amount of time taken.
- However, a variant of this bug can be used on Firefox (provided advanced tracking protection is disabled), where performance.getEntriesByName(...)[0].fetchStart - performance.getEntriesByName(...)[0].startTime can be used to detect if a URL is a redirect (the difference will be high for a redirect).

P.S: Sorry for the deleted comment spam, I didn't realize, Monorail would consider Ctrl + Enter to be a Submit action :)

Comment 5 by ajgo@google.com on Mon, Jan 24, 2022, 1:52 PM EST

**Status:** Available (was: Unconfirmed)
**Labels:** Security_Severity-Low FoundIn-96
**Components:** Internals>Network Blink>PerformanceAPIs>NavigationTiming Blink>PerformanceAPIs>ServerTiming

This repros very smoothly on Canary and I'm assuming it exists in earlier version.
Sev=Low as while this leaks some information it is fairly limited in scope.

CC'd folks could you take a look and perhaps help to route to the right person?

Comment 6 by sheriffbot on Mon, Jan 24, 2022, 2:02 PM EST

**Labels:** Security_Impact-Extended

Comment 7 by sheriffbot on Wed, Jan 26, 2022, 1:24 PM EST

**Labels:** -Pri-3 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 8 Deleted

Comment 9 by kenrb@chromium.org on Tue, Feb 8, 2022, 11:47 AM EST

**Status:** Assigned (was: Available)
**Owner:** yoavweiss@chromium.org
**Labels:** OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros

yoavweiss@: Can you please take a look at this for triage?

Comment 10 by datta...@gmail.com on Tue, Feb 8, 2022, 1:38 PM EST Project Member

Few updates (kinda) wrt to this bug:
- Reported the above mentioned bug in Firefox to Bugzilla at https://bugzilla.mozilla.org/show_bug.cgi?id=1751678 (the bug is security restricted)
- The difference of performance.now() v/s recorded startTime does not seem confined to fetch(), but rather occurs for any kind of connection that is logged by the performance API (i.e. it could be implemented using something like <iframe>, <object>, <style>, <script>, <link>, or even <img> tags)
- Based on some digging around I did on my own, I think the bug appears to be caused by the startTime being explicitly set to the request time of the final response in the Performance::GenerateResourceTiming() function in third_party/blink/renderer/core/timing/performance.cc (https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/timing/performance.cc;l=565-574;bpv=1;bpt=1?q=GenerateResourceTiming&ss=chromium%2Fchromium%2Fsrc). Removing/commenting out the block appears to/should prevent this particular kind of redirect detection since the startTime is then set to the request time of the first request and the duration is set to the difference between the start of the first request and the end of last.

P.S: I have added a PoC to this comment demonstrating how a img tag could be used to detect redirects using this bug.

[Deleted] **img_test.html**

Comment 11 by datta...@gmail.com on Wed, Feb 9, 2022, 12:15 AM EST Project Member

Attaching the PoC for the img tags, since I seemed to have sent a different version that doesn't work in the last comment.

**img_test.html**
967 bytes View Download

Comment 12 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 1:34 AM EST

Apologies for my delay here, this fell off my radar.. Looking into this, but this seems legit :/

Comment 13 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 1:46 AM EST

**Cc:** noam....@gmail.com

Adding noam@, who's working on this spec.

Comment 14 by noam....@gmail.com on Wed, Feb 9, 2022, 1:57 AM EST

Could this be related to https://bugs.chromium.org/p/chromium/issues/detail?id=1192641?

Comment 15 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 2:04 AM EST

Turns out, this is already reported in https://bugs.chromium.org/p/chromium/issues/detail?id=1192641

Comment 16 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 2:40 AM EST

https://chromium-review.googlesource.com/c/chromium/src/+/3448777

Comment 17 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 2:51 AM EST

**Cc:** npm@chromium.org

+npm@ who's reviewing the fix

Comment 18 by yoavweiss@chromium.org on Wed, Feb 9, 2022, 10:06 AM EST

**Cc:** terjanq@google.com yhirano@chromium.org dgozman@chromium.org adetaylor@chromium.org yoavweiss@chromium.org ahemery@chromium.org

~~Issue 1295227~~ has been merged into this issue.

Comment 19 by datta...@gmail.com on Wed, Feb 9, 2022, 10:32 AM EST Project Member

yoavweiss@ wrt to the patch/commit that you linked (in comment 16), you guys should probably also change/update the GenerateResourceTiming() method at content/browser/loader/object_navigation_fallback_body_loader.cc since that also appears to be explictly setting the start_time to the start of the last request in the redirect chain. (It can be triggered by loading a redirect to a error page (404/500 etc) in a <object> element)

Comment 20 by yoavweiss@chromium.org on Thu, Feb 10, 2022, 4:58 PM EST

**Cc:** toyoshim@chromium.org

dattasohom1@ - thanks for pointing that out!! Should be good now.

Comment 21 by yoavweiss@chromium.org on Fri, Feb 11, 2022, 2:18 AM EST

**Cc:** altimin@chromium.org

Comment 22 by Git Watcher on Fri, Feb 11, 2022, 9:12 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e96b9f57d8d9e32bf9cb748524735d7903271755

commit e96b9f57d8d9e32bf9cb748524735d7903271755
Author: Yoav Weiss <yoavweiss@chromium.org>
Date: Fri Feb 11 14:11:29 2022

[resource-timing] Fix failing WPT test

Bug: 1192641, ~~1290150~~
Change-Id: I70f5c662dbc7edfb52d2f9c9f2c36cc382b8210f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3448777
Reviewed-by: Nicolás Peña <npm@chromium.org>
Reviewed-by: Alexander Timin <altimin@chromium.org>
Commit-Queue: Yoav Weiss <yoavweiss@chromium.org>
Cr-Commit-Position: refs/heads/main@{#969926}

[modify]
https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/content/browser/loader/object_navigation_fallback_body_loader.cc
[modify]
https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/third_party/blink/web_tests/external/wpt/resource

https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/third_party/blink/web_tests/external/wpt/resource-timing/object-not-found-after-cross-origin-redirect.html
[modify] https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/third_party/blink/renderer/core/timing/performance_resource_timing.cc
[modify] https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/third_party/blink/web_tests/TestExpectations
[modify] https://crrev.com/e96b9f57d8d9e32bf9cb748524735d7903271755/third_party/blink/renderer/core/timing/performance.cc

Comment 23 by yoavweiss@chromium.org on Fri, Feb 11, 2022, 10:38 AM EST

**Status:** Fixed (was: Assigned)

Comment 24 by sheriffbot on Fri, Feb 11, 2022, 12:42 PM EST

**Labels:** reward-topanel

Comment 25 by sheriffbot on Fri, Feb 11, 2022, 1:41 PM EST

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

Comment 26 by datta...@gmail.com on Sat, Mar 5, 2022, 5:39 AM EST Project Member

This bug seems to have been fixed in Chrome 100 (Beta). Thanks for fixing the issue :)

Comment 27 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:59 PM EDT

**Labels:** Release-0-M100

Comment 28 by amyressler@google.com on Tue, Mar 29, 2022, 1:15 PM EDT

**Labels:** CVE-2022-1146 CVE_description-missing

Comment 29 by amyressler@google.com on Thu, Mar 31, 2022, 5:15 PM EDT

**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 30 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:54 PM EDT

Congratulations! The VRP Panel has decided to award you $1,000 for this report. A member of our finance team will be in touch to arrange payment. Thank you for your efforts and reporting this issue to us!

Comment 31 by amyressler@google.com on Fri, Apr 1, 2022, 4:15 PM EDT

**Labels:** -reward-unpaid reward-inprocess

Comment 32 by sheriffbot on Fri, May 20, 2022, 1:32 PM EDT

**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 33 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT

**Labels:** CVE_description-submitted -CVE_description-missing

Comment 34 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

**Labels:** -CVE_description-missing --CVE_description-missing