



☆ Starred by 2 users


Owner:


yoavweiss@chromium.org


CC:


 falken@chromium.org


 natashapabrai@google.com


 igng...@chromium.org


 npm@chromium.org

 mmoroz@chromium.org

 bashi@chromium.org

 sor.k...@gmail.com

 panicker@chromium.org

 yoavweiss@chromium.org

Status:

Fixed (Closed)

Components:

Blink>PerformanceAPIs

Modified:

May 20, 2020

Backlog-Rank:

----

Editors:

----

EstimatedDays:

----

NextAction:

----

OS:

Linux, Windows, Chrome, Mac, Fuchsia

Pri:

1

Type:

Bug-Security

reward-2000

Security\_Impact-Stable

Security\_Severity-Medium

M-80

allpublic

reward-inprocess

CVE\_description-submitted

Target-80

reward\_to-sor.karami\_at\_gmail.com

Release-0-M83

CVE-2020-6473

Blocking:

Issue 1047915

Issue 1049510: Unexpected reveal of service worker interception by using nextHopProtocol

Reported by shimazu@chromium.org on Thu, Feb 6, 2020, 3:52 AM EST Project Member

 Code

Context: <https://bugs.chromium.org/p/chromium/issues/detail?id=1047915#c4>

nextHopProtocol also needs to be protected by Timing-Allow-Origin.

Comment 1 by sheriffbot@chromium.org on Thu, Feb 6, 2020, 11:22 AM EST Project Member

**Labels:** Target-80 M-80

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 2 by yoavweiss@chromium.org on Mon, Feb 10, 2020, 10:55 AM EST Project Member

CC: igng...@chromium.org

Comment 3 by bugdroid on Wed, Feb 12, 2020, 6:28 AM EST Project Member

The following revision refers to this bug:  
<https://chromium.googlesource.com/chromium/src.git/+cf3e88c366ec69d74504f065daa0bdee07cf2fac>

commit cf3e88c366ec69d74504f065daa0bdee07cf2fac

Author: Yoav Weiss <yoavweiss@chromium.org>

Date: Wed Feb 12 11:27:10 2020

[resource-timing] nextHopProtocol on iframes should be TAO protected

Implements <https://github.com/w3c/resource-timing/pull/224>

**Bug-1049510**

Change-Id: Id8fc4b3a4de72b6a51c820a2352d88bea65c935f

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2047023>

Auto-Submit: Yoav Weiss <yoavweiss@chromium.org>

Commit-Queue: Yoav Weiss <yoavweiss@chromium.org>

Reviewed-by: Matt Falkenhagen <falken@chromium.org>

Reviewed-by: Ben Kelly <wanderview@chromium.org>

Reviewed-by: Annie Sullivan <sullivan@chromium.org>

Cr-Commit-Position: refs/heads/master@{#740624}

[modify] [https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third\\_party/blink/renderer/core/timing/performance\\_resource\\_timing.cc](https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third_party/blink/renderer/core/timing/performance_resource_timing.cc)

[modify] [https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third\\_party/blink/renderer/core/timing/performance\\_resource\\_timing.h](https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third_party/blink/renderer/core/timing/performance_resource_timing.h)

[modify] [https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third\\_party/blink/renderer/core/timing/performance\\_resource\\_timing\\_test.cc](https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third_party/blink/renderer/core/timing/performance_resource_timing_test.cc)

[add] [https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third\\_party/blink/web\\_tests/external/wpt/resource-timing/nextHopProtocol-tao-protected.html](https://crrev.com/cf3e88c366ec69d74504f065daa0bdee07cf2fac/third_party/blink/web_tests/external/wpt/resource-timing/nextHopProtocol-tao-protected.html)

Comment 4 by yoavweiss@chromium.org on Wed, Feb 12, 2020, 7:01 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 5 by [sheriffbot](#) on Fri, Feb 14, 2020, 7:49 PM EST Project Member

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

Comment 6 by [tsepez@chromium.org](mailto:tsepez@chromium.org) on Wed, Mar 11, 2020, 1:21 PM EDT Project Member

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

Comment 7 by [falken@chromium.org](mailto:falken@chromium.org) on Mon, Apr 27, 2020, 5:50 PM EDT Project Member

Cc: [sor.k...@gmail.com](mailto:sor.k...@gmail.com) [natashapabrai@google.com](mailto:natashapabrai@google.com)

Labels: reward-topanel

[natashapabrai](#): This bug was originally reported by [sor.karami@gmail.com](mailto:sor.karami@gmail.com) in issue 1047915. Does it need review for VRP? Adding reward-topanel in case it's eligible (if that's the right label).

Comment 8 by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, May 6, 2020, 5:53 PM EDT Project Member

Labels: reward\_to-sor.karami\_at\_gmail.com

Comment 9 by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, May 7, 2020, 12:50 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-2000

\*\*\* 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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

Comment 10 by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, May 7, 2020, 2:03 PM EDT Project Member

Congrats! The Panel decided to award \$2,000 for this report.

Comment 11 by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, May 7, 2020, 2:09 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 12 by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 13 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, May 18, 2020, 11:58 AM EDT Project Member

Labels: CVE-2020-6473 CVE\_description-missing

Comment 14 by [sheriffbot](#) on Wed, May 20, 2020, 3:01 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 15 by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, May 20, 2020, 11:43 PM EDT Project Member

Labels: -CVE\_description-missing CVE\_description-submitted