☆ Starred by 1 user

Owner:	yoavweiss@chromium.org
CC:	igrig...@chromium.org npm@chromium.org y...@yoav.ws achuith@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>SecurityFeature>CORS
Modified:	Apr 21, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
M-80
allpublic
reward-inprocess
CVE_description-submitted
Target-80
merge-merged-3987
merge-merged-80
Release-0-M80
CVE-2020-6400

Issue 1038036: Security: Cross-Origin (Partial) Status Code Leakage

Reported by takas...@shift-js.info on Fri, Dec 27, 2019, 10:25 AM EST

Code

VULNERABILITY DETAILS

`performance.getEntries()` allows us to leak status codes of cross-origin requests (with cookies).

When a request initiated by `<object data="...">` ends with 40x or 50x response, `performance.getEntries()` shows no records related to the request. When a request ends with 20x or 30x, however, `performance.getEntries()` returns records including ones for the request. This behavior makes us possible to check whether a status code of a cross-origin response indicates something wrong occured (= 40x or 50x) or not (= 20x or 30x).

For example, the following code initiates a request for `url` and outputs the kind of the status code to console.

~~~
```js
const url = 'http://example.com/';
// const url = 'http://example.com/404';
const sleep = msec => new Promise(resolve => setTimeout(resolve, msec));

performance.clearResourceTimings();
const el = document.createElement("object");

el.onload = el.onerror = async () => {
    await sleep(100);
    document.body.removeChild(el);
    console.log(performance.getEntriesByType("resource").length > 0? 'succeeded. (20x or 30x)' : 'something wrong occured. (40x or 50x)');
};
el.data = url;
el.style = "width: 0px; height: 0px;";
document.body.appendChild(el);
```
~~~

To the best of my knowledge, status codes of cross-origin responses must be hidden; sometimes it can be used to do XS-Leaks attacks (ref. https://github.com/xsleaks/xsleaks/wiki/Links). Although this kind of issues can be mitigated with `SameSite` attribute, it has a impact on sites which use `SameSite=None` for their cookies.

VERSION

Chrome Version: Version 79.0.3945.88 (Official Build) (64-bit), stable
Operating System: macOS Catalina Version 10.15.1

REPRODUCTION CASE

You can reproduce this issue with the following steps:

1. Open status.html that I attached to this report.
2. Input `http://example.com/` to the form and press "Check" button. Then you will see "status code: 2xx or 3xx".
3. Input `http://example.com/404` to the form and press "Check" button. Then you will see "status code: 4xx or 5xx".

CREDIT INFORMATION

Reporter credit: Takashi Yoneuchi (@y0n3uchy)

poc.html
2.1 KB View Download

Comment 1 by adetaylor@google.com on Sat, Dec 28, 2019, 1:33 AM EST Project Member

Owner: mkwst@chromium.org
Components: Blink>SecurityFeature>CORS

Thanks very much for the report and very clear explanation.

mkwst@, WDYT?

Comment 2 by sheriffbot@chromium.org on Sat, Dec 28, 2019, 11:17 AM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 3 by mkwst@chromium.org on Sat, Dec 28, 2019, 11:46 AM EST Project Member

Owner: y...@yoav.ws
Cc: igrig...@chromium.org

I don't know what the guarantees are we want to make around `performance.getEntries()`. Yoav or Ilya might?

Comment 4 by adetaylor@google.com on Sun, Dec 29, 2019, 11:41 AM EST Project Member

Labels: Security_Impact-Stable Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows

Thanks Mike.

I have confirmed that the POC has the behavior that the reporter describes on M79.

As a fairly minor cross-origin leak I'm not sure if this should be medium severity or low severity. I'll err on medium. But Mike, Yoav, feel free to adjust.

Thank you again for the report.

Comment 5 by sheriffbot@chromium.org on Mon, Dec 30, 2019, 9:47 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 6 by sheriffbot@chromium.org on Mon, Dec 30, 2019, 10:24 AM EST Project Member

Labels: Pri-1

Setting Pri-1 to match security severity Medium. 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 7 by y...@yoav.ws on Mon, Jan 6, 2020, 4:43 AM EST Project Member

Owner: yoavweiss@chromium.org
Cc: y...@yoav.ws npm@chromium.org

This should've been resolved with https://chromium-review.googlesource.com/c/chromium/src/+/1796544
I guess `<object>` somehow go through a different code path. I'll take a look

Comment 8 by bugdroid on Fri, Jan 10, 2020, 6:16 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/add3de3e61bdd06d217307eca97f35e38f257aa9

commit add3de3e61bdd06d217307eca97f35e38f257aa9
Author: Yoav Weiss <yoavweiss@chromium.org>
Date: Fri Jan 10 23:15:28 2020

[resource-timing] Error status code nav requests add entry to parent

In [1] we made sure that subresource requests that get a failing status
code still get their resource-timing entries reported.
However, it seems like we failed to do the same with navigation
requests that are typically reported to their parents.
This CL fixes that.

[1] https://chromium-review.googlesource.com/c/chromium/src/+/1796544

~~Bug: 1038036~~
Change-Id: I56afc1aae1b048690b8b72ac7ef58b6353fb87a6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/1994288
Commit-Queue: Yoav Weiss <yoavweiss@chromium.org>
Reviewed-by: Nicolás Peña Moreno <npm@chromium.org>
Cr-Commit-Position: refs/heads/master@{#730335}

[modify] https://crrev.com/add3de3e61bdd06d217307eca97f35e38f257aa9/third_party/blink/renderer/core/loader/document_loader.cc
[add] https://crrev.com/add3de3e61bdd06d217307eca97f35e38f257aa9/third_party/blink/web_tests/external/wpt/resource-timing/object-not-found-adds-entry.html

Comment 9 by sheriffbot@chromium.org on Sat, Jan 11, 2020, 9:10 AM EST Project Member

yoavweiss: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 10 by yoavweiss@chromium.org on Sun, Jan 12, 2020, 3:03 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 11 by sheriffbot@chromium.org on Mon, Jan 13, 2020, 10:42 AM EST Project Member

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

Comment 12 by natashapabrai@google.com on Tue, Jan 14, 2020, 11:56 AM EST Project Member

Labels: reward-topanel

Comment 13 by sheriffbot@chromium.org on Wed, Jan 15, 2020, 11:09 AM EST Project Member

Labels: Merge-Request-80

Requesting merge to beta M80 because latest trunk commit (730335) appears to be after beta branch point (722274).

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

Comment 14 by sheriffbot@chromium.org on Wed, Jan 15, 2020, 11:12 AM EST Project Member

Labels: -Merge-Request-80 Merge-Review-80 Hotlist-Merge-Review

This bug requires manual review: M80'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://goto.google.com/chrome-release-branch-merge-guidelines
- 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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.
Owners: govind@(Android), Kariahda@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 15 by srinivassista@google.com on Wed, Jan 15, 2020, 11:58 AM EST Project Member

yoavweiss@ pls help answer the questions in comment #14 for a merge review.

Comment 16 by yoavweiss@chromium.org on Thu, Jan 16, 2020, 12:29 AM EST Project Member

1) I believe we're now somewhere between phase 2 and 3. I'm not sure if this bug should be considered "release blocking", that depends on its security severity so not my call. However, the fix is of very low complexity, only impacting a single condition.
2) https://chromium-review.googlesource.com/c/chromium/src/+/1994288
3) It has landed in master. I manually verified it in Canary.
4) This change fixes a security issue which enables cross-site inspection of errored status codes. If the severity of the issue is considered "release blocking", we want to fix it even after branch point.
5) Not a new feature, but a fix for a stable one.
6) N/A

Comment 17 by srinivassista@google.com on Thu, Jan 16, 2020, 11:39 AM EST Project Member

Labels: -Merge-Review-80 Merge-Approved-80

merge approved for M80, branch:3897, pls merge your changes to the branch asap

Comment 18 by yoavweiss@chromium.org on Fri, Jan 17, 2020, 1:53 AM EST Project Member

srinivassista@ - I'm getting a "branch not found" error for 3897 (on both gerrit and drover)

Comment 19 by gov...@chromium.org on Fri, Jan 17, 2020, 10:54 AM EST Project Member

Please merge your change to M80 branch 3987 ASAP. Thank you.

Comment 20 by gov...@chromium.org on Fri, Jan 17, 2020, 11:07 AM EST Project Member

M80 merge is going thru CQ - https://chromium-review.googlesource.com/c/chromium/src/+/2007482

Comment 21 by npm@google.com on Fri, Jan 17, 2020, 11:14 AM EST Project Member

For the future you can also find the branch numbers on http://www.chromium.org/developers/how-tos/drover.

Comment 22 by bugdroid on Fri, Jan 17, 2020, 12:02 PM EST Project Member

Labels: -merge-approved-80 merge-merged-3987 merge-merged-80

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/237e4895f680e545259c01437d5ea987a9bc3eea

commit 237e4895f680e545259c01437d5ea987a9bc3eea
Author: Yoav Weiss <yoavweiss@chromium.org>
Date: Fri Jan 17 17:00:51 2020

[resource-timing] Error status code nav requests add entry to parent

In [1] we made sure that subresource requests that get a failing status
code still get their resource-timing entries reported.
However, it seems like we failed to do the same with navigation
requests that are typically reported to their parents.
This CL fixes that.

[1] https://chromium-review.googlesource.com/c/chromium/src/+/1796544

(cherry picked from commit add3de3e61bdd06d217307eca97f35e38f257aa9)

~~Bug: 1038036~~
Change-Id: I56afc1aae1b048690b8b72ac7ef58b6353fb87a6
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/1994288
Commit-Queue: Yoav Weiss <yoavweiss@chromium.org>
Reviewed-by: Nicolás Peña Moreno <npm@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#730335}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2007482
Reviewed-by: Krishna Govind <govind@chromium.org>
Reviewed-by: Yoav Weiss <yoavweiss@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#600}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/237e4895f680e545259c01437d5ea987a9bc3eea/third_party/blink/renderer/core/loader/document_loader.cc
[add] https://crrev.com/237e4895f680e545259c01437d5ea987a9bc3eea/third_party/blink/web_tests/external/wpt/resource-timing/object-not-found-adds-entry.html

Comment 23 by natashapabrai@google.com on Thu, Jan 23, 2020, 4:21 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 natashapabrai@google.com on Thu, Jan 23, 2020, 4:36 PM EST Project Member

Congrats the Panel decided to reward $1,000 for this report!

Comment 25 by natashapabrai@google.com on Thu, Jan 23, 2020, 5:04 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 26 by adetaylor@google.com on Sat, Feb 1, 2020, 8:13 PM EST Project Member

Labels: Release-0-M80

Comment 27 by adetaylor@chromium.org on Mon, Feb 3, 2020, 6:47 PM EST Project Member

Labels: CVE-2020-6400 CVE_description-missing

Comment 28 by adetaylor@chromium.org on Mon, Feb 10, 2020, 4:37 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 29 by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST Project Member

Cc: achuith@chromium.org

Comment 30 by sheriffbot on Tue, Apr 21, 2020, 2:54 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