Starred by 2 users

Owner:	mek@chromium.org
CC:	adetaylor@chromium.org asully@chromium.org jsb...@chromium.org mek@chromium.org pwnall@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Storage>FileAPI
Modified:	Sep 14, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
Target-90
merge-merged-4240
M-91
LTR-Merged-86
LTS-Security-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
merge-merged-4430_101
Release-3-M90
CVE-2021-30515

Issue 1201073: Security: UAP in FileReader

Reported by jtrro...@gmail.com on Wed, Apr 21, 2021, 2:08 AM EDT

Code

VULNERABILITY DETAILS

A FileReader instance is normally referenced in the JavaScript and/or pending_readers_/running_readers_ of FileReader::ThrottlingController in Blink heap. And there is a way to drop all references to FileReader while it's still loading data, which leads to UAF.

In FileReader::abort,
1. state_ is set to kDone
2. The abort event is dispatched to user script
3. FileReader::Terminate is called which sets state_ to kDone again

```
void FileReader::abort() {
  // ...
  state_ = kDone;             // ======> [1]

  base::AutoReset<bool> firing_events(&still_firing_events_, true);

  // Setting error implicitly makes |result| return null.
  error_ = file_error::CreateDOMException(FileErrorCode::kAbortErr);

  // Unregister the reader.
  ThrottlingController::FinishReaderType final_step =
      ThrottlingController::RemoveReader(GetExecutionContext(), this);

  FireEvent(event_type_names::kAbort);       // ======> [2]
  FireEvent(event_type_names::kLoadend);

  // All possible events have fired and we're done, no more pending activity.
  ThrottlingController::FinishReader(GetExecutionContext(), this, final_step);

  // Also synchronously cancel the loader, as script might initiate a new load
  // right after this method returns, in which case an async termination would
  // terminate the wrong loader.
  Terminate();                           // ======> [3]
}
```

https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/fileapi/file_reader.cc;l=328;drc=eb0355c2458162b6f9cd29ed8810e32814b65e78

So we can call read methods on the same FileReader in the abort event listener, because state_ has been set to kDone which could pass the check in FileReader::ReadInternal [4].

```
void FileReader::ReadInternal(Blob* blob,
                              FileReaderLoader::ReadType type,
```

```
                    ExceptionState& exception_state) {
  // If multiple concurrent read methods are called on the same FileReader,
  // InvalidStateError should be thrown when the state is kLoading.
  if (state_ == kLoading) {               // ======> [4]
    exception_state.ThrowDOMException(
        DOMExceptionCode::kInvalidStateError,
        "The object is already busy reading Blobs.");
    return;
  }
  // ...
}
```

https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/core/fileapi/file_reader.cc;l=277;drc=eb0355c2458162b6f9cd29ed8810e32814b65e78

In PoC, we firstly create 100 (kMaxOutstandingRequestsPerThread) FileReaders, then call readAsText on the already aborted FileReader (g_reader). In this case, g_reader would be pushed in pending_readers_. We then schedule a micro task to remove running FileReaders in running_readers_ by calling abort method on them so that g_reader will be executed. After the abort event listener returns, the state_ of g_reader will be set to kDone again in FileReader::Terminate, although g_reader is about to loading data.

There is a listener (progressHandler in PoC) registered for progress event, and in this function we can call readAsText on g_reader again. At this time, there are two reading requests on g_reader but only one reference is kept in running_readers_ (because running_readers_ is a HashSet, not a Queue). When the first reading task is finished, g_reader would be removed from running_readers_.

As to JavaScript world, we can drop the reference to g_reader by simply set the variable to another value. Now g_reader could be garbage collected and an UAF would occur when any async callback on the FileReader is called.

This bug should affect the current stable version of Chrome.

VERSION
Chrome Version: 90.0.4430.85 stable

REPRODUCTION CASE

1. Setup a HTTPServer
python -m SimpleHTTPServer 8000

2. Run asan build chrome, and click 'Trigger' button
./chrome --js-flags="--expose-gc" http://localhost:8000/poc.html

Note that I only tested the poc on custom build Chromium 92.0.4480.2, crash may not happen on other versions because of the uncertainty behavior of GC process, you may adjust the parameter 'n' passed to mygc function in poc to trigger the crash.

CREDIT INFORMATION

Rong Jian and Guang Gong of Alpha Lab, Qihoo 360.

poc.html
3.5 KB View Download

asan.log
17.6 KB View Download

Comment 1 by sheriffbot on Wed, Apr 21, 2021, 2:08 AM EDT

Labels: external_security_report

Comment 2 by ClusterFuzz on Wed, Apr 21, 2021, 8:56 PM EDT

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6682182970834944.

Comment 3 by carlosil@chromium.org on Thu, Apr 22, 2021, 9:54 PM EDT

Owner: verwa...@chromium.org
Labels: Security_Severity-High Security_Impact-Head OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Infra>Client>V8

verwaest: Can you help further triage this issue? Neither I nor clusterfuzz could reproduce, but the log seems like a legitimate bug. Thanks.

Comment 4 by carlosil@chromium.org on Thu, Apr 22, 2021, 10:34 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 5 by jtrro...@gmail.com on Fri, Apr 23, 2021, 12:29 AM EDT

Hi, I download and test an asan-linux-release chromium from [https://storage.googleapis.com/chromium-browser-asan/linux-release/asan-linux-release-873021.zip] ("updated": "2021-04-15T21:24:18.572Z", "cr-git-commit": "8fd8a59cd3dc1b87330cf98280984b36e33bf36d"). The PoC should works on this version too. Hope this helps to reproduce.

Comment 6 by sheriffbot on Fri, Apr 23, 2021, 12:52 PM EDT

Labels: M-92 Target-92

Setting milestone and target because of Security_Impact=Head and high severity.

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

Comment 7 by sheriffbot on Fri, Apr 23, 2021, 1:17 PM EDT

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 8 by sheriffbot on Fri, Apr 23, 2021, 1:27 PM EDT

Labels: -Pri-3 Pri-1

Setting Pri-1 to match security severity High. 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 verwa...@chromium.org on Thu, Apr 29, 2021, 4:42 AM EDT

Owner: jsb...@chromium.org
Components: -Infra>Client>V8

jsbell: Can you triage this further? This seems very much outside of my scope.

Comment 10 by ajgo@google.com on Thu, Apr 29, 2021, 11:25 AM EDT

Cc: jsb...@chromium.org mek@chromium.org pwnall@chromium.org
Labels: -Security_Impact-Head Security_Impact-Stable
Components: Blink>Storage>FileAPI

Adding some OWNERs - please take a look at this security report.

Comment 11 by jsb...@chromium.org on Thu, Apr 29, 2021, 11:31 AM EDT

Owner: mek@chromium.org
Cc: asully@chromium.org

Passing off to mek@

Comment 12 by ajgo@google.com on Thu, Apr 29, 2021, 12:34 PM EDT

Confirms this repos on Linux asan:-

==1==ERROR: AddressSanitizer: use-after-poison on address 0x7ec026de2ee0 at pc 0x559729ccbaa4 bp 0x7fbc82495ef0 sp 0x7fbc82495ee8
READ of size 8 at 0x7ec026de2ee0 thread T13 (DedicatedWorker)
==1==WARNING: invalid path to external symbolizer!
==1==WARNING: Failed to use and restart external symbolizer!
    #0 0x559729ccbaa3 (/usr/local/google/home/ajgo/chromium/src/out/asan/chrome+0x25805aa3)
    #1 0x559729ccc456 (/usr/local/google/home/ajgo/chromium/src/out/asan/chrome+0x25806456)

I cannot repro on Windows.

Comment 13 by mek@chromium.org on Thu, Apr 29, 2021, 12:37 PM EDT

I think simply moving the Terminate call to happen before any of the events are dispatched should be enough to fix this.

We should also follow up by fixing the bug that the loadend event should not be dispatched if during the abort event another load started (as per spec), but that bug shouldn't cause any security issues, it's merely a spec compliance thing.

For the general class of FileReaderLoader related UAP bugs, we also have issue 1144264 filed to track making all of this less fragile, as we seem to keep getting bitten by this. Although while that would have fixed the UAP in this specific bug, FileReader would still be in a weird internal state where state_ == kDone but a read is still in progress.

Comment 14 by mek@chromium.org on Thu, Apr 29, 2021, 2:57 PM EDT

Also note that this is a use-after-poison, not a use-after-free. Not sure if that makes the severity/impact any different, but I imagine a UAP is less exploitable than a UAF since the memory being accessed can't have been reused for anything else yet.

Comment 15 by mek@chromium.org on Thu, Apr 29, 2021, 2:58 PM EDT

Summary: Security: UAP in FileReader (was: Security: UAF in FileReader)

Comment 16 by Git Watcher on Thu, Apr 29, 2021, 3:01 PM EDT

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/a74c980df61dd7367ad1b11e6a735be82d2696f0

commit a74c980df61dd7367ad1b11e6a735be82d2696f0
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Thu Apr 29 19:00:26 2021

FileAPI: Terminate FileReaderLoader before dispatching onabort event.

Otherwise FileReader could end up in an inconsistent state where a load
is still in progress while the state was set to done.

Bug: 1201073
Change-Id: Ib2c833537e1badc57d125568d5d35f53f12582a8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2860442
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/heads/master@{#877579}

[modify] https://crrev.com/a74c980df61dd7367ad1b11e6a735be82d2696f0/third_party/blink/renderer/core/fileapi/file_reader.cc

Comment 17 by ajgo@google.com on Fri, Apr 30, 2021, 12:59 PM EDT

Thanks - please mark this bug fixed if the above CL resolves the issue - that will kick off the merge process. (security bugs are a bit weird here!)

Comment 18 by asully@chromium.org on Fri, Apr 30, 2021, 1:08 PM EDT

Status: Fixed (was: Assigned)

I imagine mek@ left this open because there's a bit of follow-up work we'd like here, but that has a separate bug (crbug.com/1204139) and the above CL resolves the UAP. This is safe to mark as fixed.

Comment 19 by sheriffbot on Fri, Apr 30, 2021, 2:02 PM EDT

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

Comment 20 by sheriffbot on Sat, May 1, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 21 by adetaylor@google.com on Mon, May 3, 2021, 4:06 PM EDT

Cc: adetaylor@chromium.org

mek@ asully@ this is currently marked as impacting only Head (i.e. M92 and later). That seems unlikely to be the case - could you confirm that this affects from M90 onwards?

Comment 22 by asully@chromium.org on Mon, May 3, 2021, 5:28 PM EDT

Yes, this impacts from at least M90 onwards

Comment 23 by adetaylor@chromium.org on Mon, May 3, 2021, 5:37 PM EDT

Labels: -ReleaseBlock-Stable -M-92 -Target-92 M-90 Target-90 Merge-Request-90 Merge-Request-91

Thanks, duly adjusting all the labels.

(Also, I realized I was wrong - this had already been corrected to Security_Impact-Stable, but all the derived downstream labels hadn't been tweaked).

Comment 24 by adetaylor@chromium.org on Mon, May 3, 2021, 5:39 PM EDT

Labels: -Merge-Request-90 -Merge-Request-91 Merge-Approved-90 Merge-Approved-91

Approving merge to M90, branch 4430, and M91, branch 4472, unless any problems have shown up in Canary.

For M90 please merge by Thursday EOD PST for next week's stable refresh.

Comment 25 by sheriffbot on Mon, May 3, 2021, 5:39 PM EDT

Labels: Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91'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: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 26 by pbommana@google.com on Tue, May 4, 2021, 7:08 AM EDT

[Bulk Edit] Your change has been approved for M91. Please go ahead and merge the CL to branch 4472 (refs/branch-heads/4472) manually asap so that it would be part of tomorrow's Beta release.

Comment 27 by pbommana@google.com on Tue, May 4, 2021, 8:10 AM EDT

Labels: -Merge-Review-91

Comment 28 by Git Watcher on Tue, May 4, 2021, 1:31 PM EDT

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/73e026b190a8afa11e3aeb9e00ffd7d387a2d919

commit 73e026b190a8afa11e3aeb9e00ffd7d387a2d919
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Tue May 04 17:30:06 2021

FileAPI: Terminate FileReaderLoader before dispatching onabort event.

Otherwise FileReader could end up in an inconsistent state where a load
is still in progress while the state was set to done.

(cherry picked from commit a74c980df61dd7367ad1b11e6a735be82d2696f0)

Bug: 1201073
Change-Id: Ib2c833537e1badc57d125568d5d35f53f12582a8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2860442
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877579}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871354
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Austin Sullivan <asully@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#730}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/73e026b190a8afa11e3aeb9e00ffd7d387a2d919/third_party/blink/renderer/core/fileapi/file_reader.cc

Comment 29 by Git Watcher on Tue, May 4, 2021, 1:55 PM EDT

Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2ed886f76f3aa42078fc0dba320295a38d795219

commit 2ed886f76f3aa42078fc0dba320295a38d795219
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Tue May 04 17:54:11 2021

FileAPI: Terminate FileReaderLoader before dispatching onabort event.

Otherwise FileReader could end up in an inconsistent state where a load
is still in progress while the state was set to done.

(cherry picked from commit a74c980df61dd7367ad1b11e6a735be82d2696f0)

Bug: 1201073
Change-Id: Ib2c833537e1badc57d125568d5d35f53f12582a8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2860442
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877579}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871355
Commit-Queue: Austin Sullivan <asully@chromium.org>
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1386}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/2ed886f76f3aa42078fc0dba320295a38d795219/third_party/blink/renderer/core/fileapi/file_reader.cc

Comment 30 by amyressler@chromium.org on Fri, May 7, 2021, 5:16 PM EDT

Labels: Release-3-M90

Comment 31 by vsavu@google.com on Mon, May 10, 2021, 9:27 AM EDT

Labels: LTS-Security-86 Merge-Request-86

Comment 32 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT

Labels: CVE-2021-30515 CVE_description-missing

Comment 33 by Git Watcher on Wed, May 12, 2021, 4:48 AM EDT

Labels: merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/00f3160d978283173aecd8babfbda9cef6df9ee5

commit 00f3160d978283173aecd8babfbda9cef6df9ee5
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Wed May 12 08:46:56 2021

FileAPI: Terminate FileReaderLoader before dispatching onabort event.

Otherwise FileReader could end up in an inconsistent state where a load
is still in progress while the state was set to done.

(cherry picked from commit a74c980df61dd7367ad1b11e6a735be82d2696f0)

(cherry picked from commit 2ed886f76f3aa42078fc0dba320295a38d795219)

Bug: 1201073
Change-Id: Ib2c833537e1badc57d125568d5d35f53f12582a8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2860442
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#877579}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871355
Commit-Queue: Austin Sullivan <asully@chromium.org>
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1386}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884067
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#19}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/00f3160d978283173aecd8babfbda9cef6df9ee5/third_party/blink/renderer/core/fileapi/file_reader.cc

Comment 34 by amyressler@google.com on Wed, May 12, 2021, 7:12 PM EDT

Labels: -reward-topanel reward-unpaid reward-7500

*** 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 35 by amyressler@chromium.org on Wed, May 12, 2021, 7:29 PM EDT

Congratulations! The VRP Panel has decided to award you $7,500 for this report. Nice work!

Comment 36 by amyressler@google.com on Mon, May 17, 2021, 2:17 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 37 by sheriffbot on Wed, May 26, 2021, 12:22 PM EDT

Labels: -M-90 M-91 Target-91

Comment 38 by adetaylor@google.com on Thu, Jun 3, 2021, 2:35 PM EDT

Labels: -Merge-Request-86 LTS-Merge-Request-86

Comment 39 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 40 by gianluca@google.com on Mon, Jun 7, 2021, 6:48 AM EDT

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 41 by Git Watcher on Mon, Jun 7, 2021, 7:43 AM EDT

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c7200e16120643e610f7270a723ddd8bba877533

commit c7200e16120643e610f7270a723ddd8bba877533
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Mon Jun 07 11:42:10 2021

FileAPI: Terminate FileReaderLoader before dispatching onabort event.

Otherwise FileReader could end up in an inconsistent state where a load
is still in progress while the state was set to done.

(cherry picked from commit a74c980df61dd7367ad1b11e6a735be82d2696f0)

Bug: 1201073
Change-Id: Ib2c833537e1badc57d125568d5d35f53f12582a8
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2860442
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877579}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883604

Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1660}
Cr-Branched-From: f29767770265191 6bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/c7200e16120643e610f7270a723ddd8bba877533/third_party/blink/renderer/core/fileapi/file_reader.cc

Comment 42 by vsavu@google.com on Mon, Jun 7, 2021, 7:55 AM EDT

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 43 by sheriffbot on Tue, Sep 14, 2021, 1:31 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