☆ Starred by 1 user

Owner:	hongchan@chromium.org **OOO (12.15-1.8)**
CC:	----
Status:	Verified *(Closed)*
Components:	Blink>WebAudio
Modified:	Nov 12, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
CVE_description-submitted
M-92
Target-92
merge-merged-4430
merge-merged-90
FoundIn-92
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
LTS-Size-Small
LTS-Complexity-Trivial
Release-2-M92
CVE-2021-30603
merge-merged-4515_132

Issue 1233564: Security: Data race in HRTFDatabaseLoader::WaitForLoaderThreadCompletion

Reported by glazunov@google.com on Tue, Jul 27, 2021, 12:42 PM EDT Project Member

Code

VULNERABILITY DETAILS

```
void HRTFDatabaseLoader::WaitForLoaderThreadCompletion() {
  if (!thread_)
    return;

  base::WaitableEvent sync;
  // TODO(alexclarke): Should this be posted as a loading task?
  PostCrossThreadTask(*thread_->GetTaskRunner(), FROM_HERE,
                      CrossThreadBindOnce(&HRTFDatabaseLoader::CleanupTask,
                                          CrossThreadUnretained(this),
                                          CrossThreadUnretained(&sync)));
  sync.Wait();
  thread_.reset();
}
```

Despite what a comment in the header file says about `WaitForLoaderThreadCompletion`, it is not thread-safe. `HRTFDatabaseLoader` objects are shared among audio contexts, so multiple audio rendering threads may call the method at the same time and then race on `unique_ptr<T>::reset()`, leading to a double-free.

VERSION
Google Chrome 92.0.4515.107 (Official Build) (x86_64)
Chromium 94.0.4578.0 (Developer Build) (64-bit)

REPRODUCTION CASE

```
<body>
<script>
createGraph = rate => {
    let context = new OfflineAudioContext(1, 1, rate);
    let constant = context.createConstantSource();
    let panner = context.createPanner();

    constant.start();

    constant.connect(panner);
    panner.connect(context.destination);

    context.suspend(0);
    context.startRendering();

    return {context, panner};
}

wait = timeout => new Promise(resolve => setTimeout(resolve, timeout));

(async () => {
  for (let rate = 3000; ; ++rate) {
    let graphs = [];
    for (let i = 0; i < navigator.hardwareConcurrency; ++i)
      graphs.push(createGraph(rate));

    await wait(1000);

    for (let graph of graphs) {
      graph.panner.panningModel =  "HRTF";
      graph.context.resume();
    }

    await wait(1000);
  }
})();
</script>
</body>
```

CREDIT INFORMATION
Sergei Glazunov of Google Project Zero

This bug is subject to a 90-day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline. The scheduled deadline is 2021-10-25.

asan.log
30.0 KB View Download

Comment 1 by mea...@chromium.org on Tue, Jul 27, 2021, 2:26 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: hongchan@chromium.org
Labels: Security_Severity-High FoundIn-92 OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Blink>WebAudio

Comment 2 by sheriffbot on Tue, Jul 27, 2021, 2:33 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 3 by hongchan@chromium.org on Tue, Jul 27, 2021, 3:15 PM EDT Project Member

glazunov@ Thanks for the repro case, Sergei!

I am not able to reproduce this with a normal ASAN build. Can you share your build args (gn) and ASAN options for the reproduction?

Comment 4 by glazunov@google.com on Wed, Jul 28, 2021, 6:43 AM EDT Project Member

I used a regular `is_asan = true is_debug = false` build, and also reproduced the issue in the latest official Chrome build. That said, this race is extremely tight and each attempt to win it takes a few seconds, so the bug takes at least five minutes to reproduce on my workstation. Alternatively, you can run the repro case under TSAN.

Comment 5 by hongchan@chromium.org on Wed, Jul 28, 2021, 11:13 AM EDT Project Member

Thanks! I'll try again on linux, and perhaps with TSAN.

Comment 6 by sheriffbot on Wed, Jul 28, 2021, 12:46 PM EDT Project Member

Labels: M-92 Target-92

Setting milestone and target because of high severity.

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

Comment 7 by hongchan@chromium.org on Wed, Jul 28, 2021, 6:14 PM EDT Project Member

- Tried to repro on Linux ASAN for ~20 minutes. No luck.
- Tried to repro on Linux TSAN for ~20 minutes. No luck.

Perhaps I need to work on the repro case to make it more aggressive.

Also - is it possible to put this repro case on CF? I'll keep trying the local reproduction, but also want to try some speculative fix. Perhaps I should ask adetaylor@?

Comment 8 by ClusterFuzz on Thu, Jul 29, 2021, 9:20 AM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5763486721048576.

Comment 9 by hongchan@chromium.org on Thu, Jul 29, 2021, 2:51 PM EDT Project Member

CF also says it's unreproducible.

My simple speculative fix would be:

```
void HRTFDatabaseLoader::WaitForLoaderThreadCompletion() {
  if (!thread_)
    return;

  base::WaitableEvent sync;
  // TODO(alexclarke): Should this be posted as a loading task?
  PostCrossThreadTask(*thread_->GetTaskRunner(), FROM_HERE,
                      CrossThreadBindOnce(&HRTFDatabaseLoader::CleanupTask,
                                          CrossThreadUnretained(this),
                                          CrossThreadUnretained(&sync)));
  sync.Wait();

  // Proposed change:
  if (thread_) {
    thread_.reset();
  }
}
```

What do you think, glazunov@?

Comment 10 by glazunov@google.com on Fri, Jul 30, 2021, 8:44 AM EDT Project Member

Not sure what's going on with CF. The process output should be much longer than five lines even if the issue couldn't be reproduced. I also added a couple extra tasks, but they're still in the CF queue after 20 hours.

Unfortunately, the proposed fix wouldn't be sufficient. The `unique_ptr` class isn't thread-safe, so we have to rely on an external thread synchronization mechanism. The issue was introduced by https://source.chromium.org/chromium/chromium/src/+/0930a7b1ed1b72bee6e583937d91a543c75f7b93, which incorrectly assumed that `thread_` couldn't be accessed from multiple threads and removed a locker from `WaitForLoaderThreadCompletion`. The fix should most likely just bring the locker back.

Comment 11 by hongchan@chromium.org on Mon, Aug 2, 2021, 11:58 AM EDT Project Member

Status: Started (was: Assigned)

I see. Thanks for the insight.

The problem is that haraken@ moved the lock to solve a mysterious problem (~~https://crbug.com/415305#c6~~) in the past so reverting the change will be likely to bring the old issue back.

Comment 12 by hongchan@chromium.org on Mon, Aug 2, 2021, 6:59 PM EDT Project Member

The change in #c10 was introduced in 2014 and the code has evolved a lot. So what I implemented is not an exact revert, but a similar idea:
https://chromium-review.googlesource.com/c/chromium/src/+/3068260
(glazunov@ - your feedback would be appreciated!)

Then I got a stack trace with sig 11 crash:

```
Received signal 11 SEGV_MAPERR 000000000000
0   Chromium Framework                  0x0000000126ffdc79 base::debug::CollectStackTrace(void**, unsigned long) + 9
1   Chromium Framework                  0x0000000126cc28e3 base::debug::StackTrace::StackTrace() + 19
2   Chromium Framework                  0x0000000126ffd9fb base::debug::(anonymous namespace)::StackDumpSignalHandler(int, __siginfo*, void*) + 2891
3   libsystem_platform.dylib            0x00007fff203d8d7d _sigtramp + 29
4   ???                                 0x0000000000000001 0x0 + 1
5   Chromium Framework                  0x000000013cf09616 blink::PannerHandler::Process(unsigned int) + 774
6   Chromium Framework                  0x000000013cf08817 blink::PannerHandler::ProcessIfNecessary(unsigned int) + 903
7   Chromium Framework                  0x000000013cdee472 blink::AudioNodeOutput::Pull(blink::AudioBus*, unsigned int) + 882
8   Chromium Framework                  0x000000013cdea82d blink::AudioNodeInput::SumAllConnections(scoped_refptr<blink::AudioBus>, unsigned int) + 989
9   Chromium Framework                  0x000000013cdeac9c blink::AudioNodeInput::Pull(blink::AudioBus*, unsigned int) + 636
10  Chromium Framework                  0x000000013cef7fef blink::OfflineAudioDestinationHandler::RenderIfNotSuspended(blink::AudioBus*, blink::AudioBus*, unsigned int) +
911
11  Chromium Framework                  0x000000013cef6888 blink::OfflineAudioDestinationHandler::DoOfflineRendering() + 1640
12  Chromium Framework                  0x000000013cefa08d base::internal::Invoker<base::internal::BindState<void (blink::OfflineAudioDestinationHandler::*)(),
scoped_refptr<blink::OfflineAudioDestinationHandler> >, void ()>::RunOnce(base::internal::BindStateBase*) + 381
13  Chromium Framework                  0x0000000126e9faa2 base::TaskAnnotator::RunTask(char const*, base::PendingTask*) + 1186
14  Chromium Framework                  0x0000000126f0b6d9
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) + 2473
15  Chromium Framework                  0x0000000126f0a277 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() + 391
16  Chromium Framework                  0x0000000126f0c702 non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() +
18
17  Chromium Framework                  0x0000000126d49d80 base::MessagePumpDefault::Run(base::MessagePump::Delegate*) + 752
18  Chromium Framework                  0x0000000126f0d52a base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta) +
1498
19  Chromium Framework                  0x0000000126e095aa base::RunLoop::Run(base::Location const&) + 2346
20  Chromium Framework                  0x0000000123a2a0a3 blink::scheduler::WorkerThread::SimpleThreadImpl::Run() + 835
21  Chromium Framework                  0x0000000127027a77 base::(anonymous namespace)::ThreadFunc(void*) + 231
22  libsystem_pthread.dylib             0x00007fff203938fc _pthread_start + 224
23  libsystem_pthread.dylib             0x00007fff2038f443 thread_start + 15
[end of stack trace]
```

FYI, I don't get this crash from ToT. So I guess this crash can be fixed by removing locker from |thread_|. (i.e.
https://source.chromium.org/chromium/chromium/src/+/0930a7b1ed1b72bee6e583937d91a543c75f7b93)

Comment 13 by Git Watcher on Tue, Aug 3, 2021, 9:26 PM EDT Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src/+/6811e850ee10847da16c4d5fdc0f845494586b65

commit 6811e850ee10847da16c4d5fdc0f845494586b65
Author: Hongchan Choi <hongchan@chromium.org>
Date: Wed Aug 04 01:25:36 2021

Protect HRTF database loader thread from access by different threads

This patch add a new mutex locker around the HRTF database loader
thread to ensure the safe exclusive access of the loader thread
and the HRTF database.

~~Bug: 1233564~~
Change-Id: Ie12b99ffe520d3747e34af387a37637a10aab38a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3068260
Auto-Submit: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Cr-Commit-Position: refs/heads/master@{#908269}

[modify] https://crrev.com/6811e850ee10847da16c4d5fdc0f845494586b65/third_party/blink/renderer/platform/audio/hrtf_database_loader.cc
[modify] https://crrev.com/6811e850ee10847da16c4d5fdc0f845494586b65/third_party/blink/renderer/platform/audio/hrtf_database_loader.h

Comment 14 by hongchan@chromium.org on Wed, Aug 4, 2021, 11:39 AM EDT Project Member

Status: Verified (was: Started)

CF is still not able to reproduce, but the patch is verified by glazunov@:
https://chromium-review.googlesource.com/c/chromium/src/+/3068260/4#message-d6f7acd660eba8c19f425dbc7ddc389c097269b0

Comment 15 by sheriffbot on Wed, Aug 4, 2021, 1:41 PM EDT Project Member

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

Comment 16 by sheriffbot on Wed, Aug 4, 2021, 2:06 PM EDT Project Member

Labels: Merge-Request-92 Merge-Request-93

Requesting merge to stable M92 because latest trunk commit (908269) appears to be after stable branch point (885287).

Requesting merge to beta M93 because latest trunk commit (908269) appears to be after beta branch point (902210).

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

Comment 17 by sheriffbot on Wed, Aug 4, 2021, 2:09 PM EDT Project Member

Labels: -Merge-Request-93 Hotlist-Merge-Review Merge-Review-93

This bug requires manual review: M93'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/+/main/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), govind@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 18 by hongchan@chromium.org on Wed, Aug 4, 2021, 5:29 PM EDT Project Member

1. Yes. This is Security_Severity-High.
2. https://chromium-review.googlesource.com/c/chromium/src/+/3068260
3. Yes.
4. Yes.
5. This issue is Security_Severity-High.
6. No.
7. N/A

Comment 19 by hongchan@chromium.org on Wed, Aug 4, 2021, 5:34 PM EDT Project Member

The merge CL is ready for review:
https://chromium-review.googlesource.com/c/chromium/src/+/3072700

Comment 20 by amyressler@google.com on Mon, Aug 9, 2021, 10:32 AM EDT Project Member

Labels: -Merge-Request-92 -Merge-Review-93 Merge-Approved-93 Merge-Approved-92

Hi hongchan@, merge approved for M92 and M93. Please go ahead and merge to branches 4515 and 4577 respectively asap. Please do be sure to merge to branch 4577 by COB tomorrow, Tuesday 10 August so that this fix can be in the M93 stable cut this week. Thank you!

Comment 21 by hongchan@chromium.org on Mon, Aug 9, 2021, 12:00 PM EDT Project Member

M92 cherry pick: https://crrev.com/c/3072700
M93 cherry pick: https://crrev.com/c/3082114

amyressler@ Could you +1 these merges?

Comment 22 by gov...@chromium.org on Mon, Aug 9, 2021, 1:49 PM EDT Project Member

Please merge your change to M93 branch 4577 ASAP so we can take it in for this week Beta Release. Thank you.

Comment 23 by Git Watcher on Mon, Aug 9, 2021, 2:27 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e837bee8d83686969a3a1bcc300817e2cc21b90c

commit e837bee8d83686969a3a1bcc300817e2cc21b90c
Author: Hongchan Choi <hongchan@chromium.org>
Date: Mon Aug 09 18:25:50 2021

Protect HRTF database loader thread from access by different threads

This patch add a new mutex locker around the HRTF database loader
thread to ensure the safe exclusive access of the loader thread
and the HRTF database.

(cherry picked from commit 6811e850ee10847da16c4d5fdc0f845494586b65)

~~Bug: 1233564~~
Change-Id: Ie12b99ffe520d3747e34af387a37637a10aab38a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3068260
Auto-Submit: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#908269}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3072700
Reviewed-by: Chris Mumford <cmumford@google.com>
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#1996}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/e837bee8d83686969a3a1bcc300817e2cc21b90c/third_party/blink/renderer/platform/audio/hrtf_database_loader.cc
[modify] https://crrev.com/e837bee8d83686969a3a1bcc300817e2cc21b90c/third_party/blink/renderer/platform/audio/hrtf_database_loader.h

Comment 24 by Git Watcher on Mon, Aug 9, 2021, 2:44 PM EDT Project Member

Labels: -merge-approved-93 merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/033f0bdcbe538c61f532e97b03cb9c092a94b413

commit 033f0bdcbe538c61f532e97b03cb9c092a94b413
Author: Hongchan Choi <hongchan@chromium.org>
Date: Mon Aug 09 18:43:22 2021

Protect HRTF database loader thread from access by different threads

This patch add a new mutex locker around the HRTF database loader
thread to ensure the safe exclusive access of the loader thread
and the HRTF database.

(cherry picked from commit 6811e850ee10847da16c4d5fdc0f845494586b65)

~~Bug: 1233564~~
Change-Id: Ie12b99ffe520d3747e34af387a37637a10aab38a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3068260
Auto-Submit: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#908269}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3082114
Reviewed-by: Chris Mumford <cmumford@google.com>
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4577@{#601}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/033f0bdcbe538c61f532e97b03cb9c092a94b413/third_party/blink/renderer/platform/audio/hrtf_database_loader.cc
[modify] https://crrev.com/033f0bdcbe538c61f532e97b03cb9c092a94b413/third_party/blink/renderer/platform/audio/hrtf_database_loader.h

Comment 25 by amyressler@google.com on Mon, Aug 16, 2021, 10:11 AM EDT Project Member

Labels: Release-2-M92

Comment 26 by amyressler@google.com on Mon, Aug 16, 2021, 10:20 AM EDT Project Member

Labels: CVE-2021-30603 CVE_description-missing

Comment 27 by rzanoni@google.com on Tue, Aug 17, 2021, 8:19 AM EDT Project Member

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 28 by rzanoni@google.com on Thu, Aug 19, 2021, 11:32 AM EDT Project Member

Labels: LTS-Size-Small LTS-Complexity-Trivial

Comment 29 by gianluca@google.com on Fri, Aug 20, 2021, 3:31 AM EDT Project Member

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 30 by Git Watcher on Fri, Aug 20, 2021, 1:20 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ba7a4d0217412c58477362c5eb8e11b277ae961f

commit ba7a4d0217412c58477362c5eb8e11b277ae961f
Author: Hongchan Choi <hongchan@chromium.org>
Date: Fri Aug 20 17:19:58 2021

[M90-LTS] Protect HRTF database loader thread from access by different threads

This patch add a new mutex locker around the HRTF database loader
thread to ensure the safe exclusive access of the loader thread
and the HRTF database.

(cherry picked from commit 6811e850ee10847da16c4d5fdc0f845494586b65)

~~Bug: 1233564~~
Change-Id: Ie12b99ffe520d3747e34af387a37637a10aab38a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3068260
Auto-Submit: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Kentaro Hara <haraken@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#908269}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3097764
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1568}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/ba7a4d0217412c58477362c5eb8e11b277ae961f/third_party/blink/renderer/platform/audio/hrtf_database_loader.cc
[modify] https://crrev.com/ba7a4d0217412c58477362c5eb8e11b277ae961f/third_party/blink/renderer/platform/audio/hrtf_database_loader.h

Comment 31 by rzanoni@google.com on Mon, Aug 23, 2021, 4:09 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 32 by amyressler@google.com on Thu, Aug 26, 2021, 1:44 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 33 by Git Watcher on Tue, Sep 21, 2021, 10:23 AM EDT Project Member

Labels: merge-merged-4515_132

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6f9d0f0e2c86440bdcfde5e41917634834aebd47

commit 6f9d0f0e2c86440bdcfde5e41917634834aebd47
Author: Hongchan Choi <hongchan@chromium.org>
Date: Tue Sep 21 14:22:12 2021

Protect HRTF database loader thread from access by different threads

This patch add a new mutex locker around the HRTF database loader
thread to ensure the safe exclusive access of the loader thread
and the HRTF database.

(cherry picked from commit 6811e850ee10847da16c4d5fdc0f845494586b65)

(cherry picked from commit e837bee8d83686969a3a1bcc300817e2cc21b90c)

~~Bug: 1233564~~
Change-Id: Ie12b99ffe520d3747e34af387a37637a10aab38a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3068260
Auto-Submit: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#908269}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3072700
Reviewed-by: Chris Mumford <cmumford@google.com>
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4515@{#1996}
Cr-Original-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3172191
Auto-Submit: Joe Tessler <jrt@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515_132@{#7}
Cr-Branched-From: 8e089f9dc0d240f50afd19b527a90447b90ca5bb-refs/branch-heads/4515@{#1934}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/6f9d0f0e2c86440bdcfde5e41917634834aebd47/third_party/blink/renderer/platform/audio/hrtf_database_loader.h
[modify] https://crrev.com/6f9d0f0e2c86440bdcfde5e41917634834aebd47/third_party/blink/renderer/platform/audio/hrtf_database_loader.cc

Comment 34 by sheriffbot on Fri, Nov 12, 2021, 1:31 PM EST 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