☆ Starred by 2 users

Owner:	rtoy@chromium.org **Email to this user bounced**
CC:	adetaylor@chromium.org hongchan@chromium.org
Status:	Verified *(Closed)*
Components:	Blink>WebAudio
Modified:	Jun 26, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
M-80
Security_Severity-High
allpublic
CVE_description-submitted
Target-80
merge-merged-3987
merge-merged-80
merge-merged-4044
merge-merged-81
Release-6-M80
CVE-2020-6450

Issue 1062247: Incomplete fix of 1055788 and 1057627

Reported by m...@semmle.com on Tue, Mar 17, 2020, 8:54 AM EDT

Code

VULNERABILITY DETAILS

I'm terribly sorry about this, as the fix I suggested for 1055788 and 1057627 did not fix the problem completely and it is still possible to trigger UaP in those cases, although the fix did prevent UaF.

The fix in those issues prevents UaF of BaseAudioContext by making the AudioHandlers in the relevant callbacks (AudioScheduledSourceHandler::NotifyEnded and IIRFilterHandler::NotifyBadState) weak pointers. Take IIRFilterHandler::NotifyBadState for example:

```
@@ -105,9 +105,9 @@
     if (HasNonFiniteOutput()) {
       did_warn_bad_filter_state_ = true;

-      PostCrossThreadTask(*task_runner_, FROM_HERE,
-                          CrossThreadBindOnce(&IIRFilterHandler::NotifyBadState,
-                                              WrapRefCounted(this)));
+      PostCrossThreadTask(
+          *task_runner_, FROM_HERE,
+          CrossThreadBindOnce(&IIRFilterHandler::NotifyBadState, AsWeakPtr()));
     }
   }
 }
```

This prevents IIRFilterHandler from outliving BaseAudioContext as a cross thread task. As explained in 1055788, in order to destroy BaseAudioContext while IIRFilterHandler::NotifyBadState is waiting in the task queue, the IIRFilterNode that owns the IIRFilterHandler first needs to be destroyed, and this can only happen while the graph is being pulled, otherwise you won't arrive at the code that posts IIRFilterHandler::NotifyBadState. This will cause the ownership of IIRFilterHandler to be transferred to |rendering_orphan_handlers_| in DeferredTaskHandlers. [1]

When BaseAudioContext is *destroyed*, it clears itself out of the handlers in |rendering_orphan_handlers_| by calling DeferredTaskHandler::ContextWillBeDestroyed in the destructor [2].

```
void DeferredTaskHandler::ContextWillBeDestroyed() {
  for (auto& handler : rendering_orphan_handlers_)
    handler->ClearContext();
  for (auto& handler : deletable_orphan_handlers_)
    handler->ClearContext();
  ClearHandlersToBeDeleted();
  // Some handlers might live because of their cross thread tasks.
}
```

This means that to cause a UaF of AudioHandler using BAC after it is destroyed, the AudioHandler needs to be removed from |rendering_orphan_handlers_| at this point to prevent |context_| from being cleared. In the test cases of 1055788 and 1057627, this was done by first destroying the ExecutionContext and cause BaseAudioContext::Uninitialize to run, which calls ClearHandlersToBeDeleted to be called to clear out |rendering_orphan_handlers_|.

By making the callbacks holding weak pointers instead of scoped_refptr, the fix ensures that |rendering_orphan_handlers_| is the sole owner of the AudioHandlers after AudioNode is disposed of and hence the AudioHandlers cannot outlive BaseAudioContext. (because when BaseAudioContext is destroyed, it clears

|rendering_orphan_handlers_|, causing the handlers to be destroyed) This prevents UaF of BAC from happening.

Use-after-poison, however, can still happen after the object is GCed and before it is destroyed (when destructor is called). As the BAC only cleans itself up from |rendering_orphan_handlers_| and |deletable_orphan_handlers_| when it is destroyed, by triggering the callbacks in the window after BAC is garbage collected and before it is destroyed (destructor called), it is still possible to cause UaP. At this point, |rendering_orphan_handlers_| will still be keeping the AudioHandler alive while the AudioHandler still holds BAC as an UntraceMember, but because BAC is already garbage collected, a UaP will happen when the callback is run and trying to access BAC by calling Context()->GetExecutionContext():

```
void IIRFilterHandler::NotifyBadState() const {
  DCHECK(IsMainThread());
  if (!Context() || !Context()->GetExecutionContext()) //<-- UaP can still happen when Context()->GetExecutionContext is accessed.
    return;
  ....
```

To prevent this, and other cases that are fixed here: https://source.chromium.org/chromium/chromium/src/+/b75436e554d54b2d8d3590d7e61607e1ce67a2fe?originalUrl=https:%2F%2Fcs.chromium.org%2F I'd suggest adding a prefinalizer to BaseAudioContext and clean itself up from |rendering_orphan_handlers_| and |deletable_orphan_handlers_| there:

```
void BaseAudioContext::Dispose() {
  for (auto& handler : rendering_orphan_handlers_)
    handler->ClearContext();
  for (auto& handler : deletable_orphan_handlers_)
    handler->ClearContext();
}
```

as AudioHandler should not hold on to a reference of BaseAudioContext after it is garbage collected, this should have little side effect. The previous fixes in those issues, however, are still necessary to prevent UaF and should not be removed.

Thank you very much for your help and please let me know if there is anything that I can help. Once again, I'm terribly sorry about the oversight and that the fix I suggested was incomplete.

1.
https://source.chromium.org/chromium/chromium/src/+/129460b86794115e96b5ec4ee724f7ac971d1f41:third_party/blink/renderer/modules/webaudio/audio_node.cc;l=619;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F
2.
https://source.chromium.org/chromium/chromium/src/+/129460b86794115e96b5ec4ee724f7ac971d1f41:third_party/blink/renderer/modules/webaudio/base_audio_context.cc;l=112;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F

VERSION
Chrome version: master branch build 3bdff94, asan build 80.3987.132
Operating System: Ubuntu 18.04

REPRODUCTION CASE
The test case is a modification of the one used in 1057627 as it is easier to trigger it in that case. Place the attached stop2_poison.html and stop1.html in the same directory and serve it on localhost, then open stop2_poison.html with an asan build of Chromium.

```
./out/asan/chrome --user-data-dir=/tmp
```

As this test case relies on memory pressure to trigger GC (it is necessary to trigger GC this way as it allows the collection and destruction of BaseAudioContext to happen in separate cycles to provide the window for UaP, whereas the gc function will trigger collection and destruction on the same cycle) this may depend on the machine, so please let me know if there is problem reproducing the issue.

This has been tested on master branch 3bdff94 and 80.0.3987.132, although the fixes of 1055788 and 1057627 had not been checked in for 80.0.3987.132 and it is hard to tell if it is the previous issue that is triggering.

CREDIT INFORMATION
Reporter credit: Man Yue Mo of Github Security Lab

stop2_poison.html
810 bytes View Download

stop1.html
582 bytes View Download

asan
4.5 KB View Download

Comment 1 by est...@chromium.org on Tue, Mar 17, 2020, 3:39 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: hongchan@chromium.org
Labels: Security_Impact-Stable Security_Severity-High OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows
Components: Blink>WebAudio

hongchan@, can you please take a look?

Comment 2 by rtoy@chromium.org on Tue, Mar 17, 2020, 3:48 PM EDT Project Member

Test case uploaded to clusterfuzz: https://clusterfuzz.com/testcase-detail/4896599527456768

Comment 3 by rtoy@chromium.org on Tue, Mar 17, 2020, 4:34 PM EDT Project Member

Hmm. Clusterfuzz doesn't seem to be able to reproduce. But I can locally on my linux box. I took your suggested fix (with modifications because BaseAudioContext can't touch rendering_orphan_handlers directly). See the tentative CL https://chromium-review.googlesource.com/c/chromium/src/+/2107806

Unfortunately, this still crashes with the same backtrace for me.

Comment 4 by rtoy@chromium.org on Tue, Mar 17, 2020, 6:17 PM EDT Project Member

Made a mistake in the test case and forgot to rename a file. I'll upload a new test.

This doesn't reproduce on a mac asan build for me.

Comment 5 by rtoy@chromium.org on Tue, Mar 17, 2020, 6:46 PM EDT Project Member

Aargh. Now I can't reproduce the issue anymore. All that happened in between is that my linux box got rebooted (because I had to reboot in a few hours any way).

Comment 6 by rtoy@chromium.org on Tue, Mar 17, 2020, 6:56 PM EDT Project Member

Because I forgot to restart my webserver that serves up the tests for me. Everything is harder when it's all remote.

Comment 7 by m...@semmle.com on Wed, Mar 18, 2020, 3:50 AM EDT

Thanks for looking into this. Re comment #3, You need to use the macro USING_PRE_FINALIZER to indicate that Dispose is a prefinalize method, so this needs to be added:

```
class MODULES_EXPORT BaseAudioContext
```

```
    : public EventTargetWithInlineData,
      public ActiveScriptWrappable<BaseAudioContext>,
      public ExecutionContextLifecycleStateObserver,
      public InspectorHelperMixin {
  USING_GARBAGE_COLLECTED_MIXIN(BaseAudioContext);
  DEFINE_WRAPPERTYPEINFO();
+  USING_PRE_FINALIZER(BaseAudioContext, Dispose);   //<--- needs to add the USING_PRE_FINALIZER macro
```

and also Dispose does not need to be virtual.

Sorry about not being clear with the prefinalizer and once again, sorry about the mistake made in the fix in the first place.

Comment 8 by rtoy@chromium.org on Wed, Mar 18, 2020, 11:06 AM EDT Project Member

Owner: rtoy@chromium.org
Cc: hongchan@chromium.org

Oh, sorry, I missed the part about prefinalizer. I'm running the test now. Looks good.

Thanks so much for your help in finding the issue and also in providing a solution!

Comment 9 by sheriffbot on Wed, Mar 18, 2020, 12:49 PM EDT Project Member

Labels: Target-80 M-80

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

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

Comment 10 by sheriffbot on Wed, Mar 18, 2020, 1:30 PM EDT Project Member

Labels: 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 11 by bugdroid on Thu, Mar 19, 2020, 5:59 PM EDT Project Member

The following revision refers to this bug:
  https://chromium.googlesource.com/chromium/src.git/+/db71a0afc1d0803d6d0827fb4fa175689df8200c

commit db71a0afc1d0803d6d0827fb4fa175689df8200c
Author: Raymond Toy <rtoy@chromium.org>
Date: Thu Mar 19 21:54:36 2020

Clear context from orphan handlers when BaseAudioContext is going away

When preparing to collect a BaseAudioContext, go through all the
rendering_orphan_handlers_ and deletable_orphan_handlers_ and remove
the context from the handler. This ensures that these handlers no
longer have references to the context when the BaseAudioContext is
destroyed because in some cases, these orphan handlers will get pulled
and access the context, which is already gone.

Clearing these in a prefinalizer ensures these orphan handlers don't
try to touch the context.

Manually verified that the repro case no longer reproduces.

~~Bug: 1062247~~
Change-Id: I50d083743903eb9544e09aa1ee912fc880331501
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2107806
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/heads/master@{#751814}

[modify] https://crrev.com/db71a0afc1d0803d6d0827fb4fa175689df8200c/third_party/blink/renderer/modules/webaudio/base_audio_context.cc
[modify] https://crrev.com/db71a0afc1d0803d6d0827fb4fa175689df8200c/third_party/blink/renderer/modules/webaudio/base_audio_context.h
[modify] https://crrev.com/db71a0afc1d0803d6d0827fb4fa175689df8200c/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/db71a0afc1d0803d6d0827fb4fa175689df8200c/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 12 by m...@semmle.com on Fri, Mar 20, 2020, 8:39 AM EDT

Thanks for the fix.

I've manually applied the patch on top of 3bdff94 and tested it multiple times. I can verify that the fix is working as intended and is clearing out the raw BAC from the handlers to prevent the bug (as opposed to timing change etc. that stop the test case from working) Hopefully this will resolve all these issues completely. Thanks!

Comment 13 by rtoy@chromium.org on Fri, Mar 20, 2020, 11:38 AM EDT Project Member

Status: Verified (was: Assigned)

And thank you very much for the excellent analysis and solution!

Marking this as verified.

Comment 14 by rtoy@chromium.org on Fri, Mar 20, 2020, 11:39 AM EDT Project Member

I'll let this bake over the weekend and see if we need to merge this to earlier releases.

Comment 15 by sheriffbot on Fri, Mar 20, 2020, 2:00 PM EDT Project Member

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

Comment 16 by sheriffbot on Fri, Mar 20, 2020, 2:20 PM EDT Project Member

Labels: Merge-Request-81 Merge-Request-80

Requesting merge to stable M80 because latest trunk commit (751814) appears to be after stable branch point (989).

Requesting merge to beta M81 because latest trunk commit (751814) appears to be after beta branch point (737173).

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

Comment 17 by sheriffbot on Fri, Mar 20, 2020, 2:24 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: Request affecting a post-stable build
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 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: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 18 by rtoy@chromium.org on Fri, Mar 20, 2020, 5:12 PM EDT Project Member

1. Does your merge fit within the Merge Decision Guidelines?
Yes
2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2107806. Has the change landed and been verified on master/ToT?
3. Has the change landed and been verified on master/ToT?
Yes
4. Why are these changes required in this milestone after branch?
Security issue
5. Is this a new feature?
No
6. If it is a new feature, is it behind a flag using finch?
N/A

Since the fixes for ~~issue 1055788~~ and ~~issue 1057627~~ were not quite complete and since this should fix the rest of the problems, we should probably merge this to the same set of release as those issues.

Comment 19 by gov...@chromium.org on Fri, Mar 20, 2020, 7:44 PM EDT Project Member

Cc: adetaylor@chromium.org

+adetaylor@ (Security TPM) for M80 and M81 merge review

Comment 20 by adetaylor@google.com on Mon, Mar 23, 2020, 2:04 PM EDT Project Member

Labels: -Merge-Request-80 -Merge-Review-81 Merge-Approved-80 Merged-Approved-81

Yes, let's merge to M80 (branch 3987) and M81 (branch 4044), assuming that per #c14 nothing weird has shown up over the weekend.

Comment 21 by rtoy@chromium.org on Mon, Mar 23, 2020, 3:01 PM EDT Project Member

There are only a handful of reports of crashes for blink::AudioScheduledSourceHandler::NotifyEnded, and they're all from M80 or earlier.

I think we're ready.

Comment 22 by adetaylor@chromium.org on Mon, Mar 23, 2020, 4:06 PM EDT Project Member

Great, please merge.

Comment 23 by bugdroid on Mon, Mar 23, 2020, 4:56 PM EDT Project Member

Labels: merge-merged-81 merge-merged-4044

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/595564563bc42c27bd2efde795e7b68e75cfa660

commit 595564563bc42c27bd2efde795e7b68e75cfa660
Author: Raymond Toy <rtoy@chromium.org>
Date: Mon Mar 23 20:55:44 2020

Clear context from orphan handlers when BaseAudioContext is going away

When preparing to collect a BaseAudioContext, go through all the
rendering_orphan_handlers_ and deletable_orphan_handlers_ and remove
the context from the handler. This ensures that these handlers no
longer have references to the context when the BaseAudioContext is
destroyed because in some cases, these orphan handlers will get pulled
and access the context, which is already gone.

Clearing these in a prefinalizer ensures these orphan handlers don't
try to touch the context.

Manually verified that the repro case no longer reproduces.

(cherry picked from commit db71a0afc1d0803d6d0827fb4fa175689df8200c)

~~Bug: 1062247~~
Change-Id: I50d083743903eb9544e09aa1ee912fc880331501
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2107806
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#751814}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2116326
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/4044@{#827}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/595564563bc42c27bd2efde795e7b68e75cfa660/third_party/blink/renderer/modules/webaudio/base_audio_context.cc
[modify] https://crrev.com/595564563bc42c27bd2efde795e7b68e75cfa660/third_party/blink/renderer/modules/webaudio/base_audio_context.h
[modify] https://crrev.com/595564563bc42c27bd2efde795e7b68e75cfa660/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/595564563bc42c27bd2efde795e7b68e75cfa660/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 24 by rtoy@chromium.org on Mon, Mar 23, 2020, 5:25 PM EDT Project Member

I'll merge to M80 tomorrow, just in case something really bad happened in the M81 merge.

If that's ok.

Comment 25 by adetaylor@chromium.org on Mon, Mar 23, 2020, 5:34 PM EDT Project Member

Sounds perfect. Thanks. In fact you can do it any time up till Thursday, as we'll be cutting the M80 stable refresh branch on Friday. (This plan may change of course. Right now every plan always changes...)

Comment 26 by rtoy@chromium.org on Tue, Mar 24, 2020, 11:19 AM EDT Project Member

No new crashes on crash.corp, so I'll merge to M80 in a few minutes.

Comment 27 by rtoy@chromium.org on Tue, Mar 24, 2020, 11:21 AM EDT Project Member

Or not. There's a conflict (surprisingly) so this will take a bit longer.

Comment 28 by adetaylor@chromium.org on Tue, Mar 24, 2020, 11:37 AM EDT Project Member

OK. There was at least one other WebAudio fix we didn't merge back because it had a conflict as well. If that turns out to be the source of the conflict, we can probably merge that too - let me know what you think is best.

Comment 29 by adetaylor@chromium.org on Tue, Mar 24, 2020, 11:38 AM EDT Project Member

Labels: -Merged-Approved-81

Comment 30 by rtoy@chromium.org on Tue, Mar 24, 2020, 11:57 AM EDT Project Member

Do you happen to know which one couldn't be merged?

Comment 31 by adetaylor@chromium.org on Tue, Mar 24, 2020, 12:04 PM EDT Project Member

https://bugs.chromium.org/p/chromium/issues/detail?id=1043446#c40 is the one I'm thinking of.

Comment 32 by rtoy@chromium.org on Tue, Mar 24, 2020, 12:25 PM EDT Project Member

Ah, thanks. Looks like that CL would have worked except a conflicting comment changed. The offending CL is https://chromium-review.googlesource.com/c/chromium/src/+/1903894 which looks like it landed in 81 but wasn't merged to 80 since it wasn't a security issue.

I can work on merging CL 1034336 if you want to take that into M80. (I'll have to read docs on how to do this; it's been a long time since I handled a cherry pick with conflict.)

Comment 33 by adetaylor@google.com on Tue, Mar 24, 2020, 1:15 PM EDT Project Member

I'd certainly like to take ~~issue 1034336~~ into M80 as well, if you're having to figure out how to merge with conflicts anyway? I'll put merge-approved-80 over on that bug too.

Comment 34 by rtoy@chromium.org on Tue, Mar 24, 2020, 4:25 PM EDT Project Member

For the record, it's issue 1043446, NOT 1034336. I keep clicking the link and get taken to a totally different issue, not related to WebAudio at all.

Comment 35 by rtoy@chromium.org on Tue, Mar 24, 2020, 4:31 PM EDT Project Member

Huh. I must have used the wrong CL for the cherry pick. If I use the original CL, there are no conflicts, and the CL is ready to merge to M80 (3987): https://chromium-review.googlesource.com/c/chromium/src/+/2116585

Comment 36 by bugdroid on Tue, Mar 24, 2020, 6:35 PM EDT 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/+/b251e5d04acc3b4baf638fd0f2fffcfe68d179e1

commit b251e5d04acc3b4baf638fd0f2fffcfe68d179e1
Author: Raymond Toy <rtoy@chromium.org>
Date: Tue Mar 24 22:33:18 2020

Clear context from orphan handlers when BaseAudioContext is going away

When preparing to collect a BaseAudioContext, go through all the
rendering_orphan_handlers_ and deletable_orphan_handlers_ and remove
the context from the handler. This ensures that these handlers no
longer have references to the context when the BaseAudioContext is
destroyed because in some cases, these orphan handlers will get pulled
and access the context, which is already gone.

Clearing these in a prefinalizer ensures these orphan handlers don't
try to touch the context.

Manually verified that the repro case no longer reproduces.

(cherry picked from commit db71a0afc1d0803d6d0827fb4fa175689df8200c)

~~Bug: 1062247~~
Change-Id: I50d083743903eb9544e09aa1ee912fc880331501
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2107806
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#751814}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2116585
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1024}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/b251e5d04acc3b4baf638fd0f2fffcfe68d179e1/third_party/blink/renderer/modules/webaudio/base_audio_context.cc
[modify] https://crrev.com/b251e5d04acc3b4baf638fd0f2fffcfe68d179e1/third_party/blink/renderer/modules/webaudio/base_audio_context.h
[modify] https://crrev.com/b251e5d04acc3b4baf638fd0f2fffcfe68d179e1/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/b251e5d04acc3b4baf638fd0f2fffcfe68d179e1/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 37 by rtoy@chromium.org on Thu, Mar 26, 2020, 4:47 PM EDT Project Member

Note to self: I think we're done here and everything has been merged as needed and there isn't more to do.

Comment 38 by adetaylor@google.com on Mon, Mar 30, 2020, 1:30 PM EDT Project Member

Labels: Release-6-M80

Comment 39 by adetaylor@chromium.org on Mon, Mar 30, 2020, 6:00 PM EDT Project Member

Labels: CVE-2020-6450 CVE_description-missing

Comment 40 by adetaylor@chromium.org on Tue, Apr 14, 2020, 3:14 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 41 by sheriffbot on Fri, Jun 26, 2020, 2:59 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

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy