




☆ Starred by 1 user

Owner:	 <a href="#">rtroy@chromium.org</a> Email to this user bounced
CC:	<a href="#">adetaylor@chromium.org</a>  <a href="#">prashanthpola@chromium.org</a> <a href="#">pbomm...@chromium.org</a>  <a href="#">hongchan@chromium.org</a> <a href="#">achuith@chromium.org</a>
Status:	Verified (Closed)
Components:	<a href="#">Blink&gt;WebAudio</a>
Modified:	Jun 10, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	<a href="#">Linux</a> , <a href="#">Android</a> , <a href="#">Windows</a> , <a href="#">Chrome</a> , <a href="#">Mac</a>
Pri:	1
Type:	<a href="#">Bug-Security</a>
<a href="#">Hotlist-Merge-Review</a> <a href="#">Security_Impact-Stable</a> <a href="#">M-80</a> <a href="#">Security_Severity-High</a> <a href="#">allpublic</a> <a href="#">CVE_description-submitted</a> <a href="#">Target-80</a> <a href="#">VulnerabilityAnalysis-Requested</a> <a href="#">merge-merged-3987</a> <a href="#">merge-merged-80</a> <a href="#">merge-merged-4044</a> <a href="#">merge-merged-81</a> <a href="#">CVE-2020-6428</a> <a href="#">merge-merged-3987_137</a> <a href="#">Release-5-M80</a>	

Issue 1057593: UaF in DeferredTaskHandler::BreakConnections

Reported by [m...@semmle.com](#) on Mon, Mar 2, 2020, 7:00 AM EST

🔗 Code

VULNERABILITY DETAILS

When `HandlePreRenderTask` is called during the rendering, it will check whether any source node should be stopped[1]. If an `AudioScheduleSourceNode`, (e.g. `ConstantSourceNode`) is to be stopped at or before the frame [2], it will then call the `AudioScheduledSourceHandler::Finish()` method, which calls `FinishWithoutOnEnded`. This has 2 effects:

1. It calls `BaseAudioContext::NotifySourceNodeFinishedProcessing`[3], which will add the `AudioScheduledSourceHandler` in the `[finished_source_handlers_]` vector, as raw pointer.

```
void BaseAudioContext::NotifySourceNodeFinishedProcessing(
    AudioHandler* handler) {
    DCHECK(!IsAudioThread());

    GetDeferredTaskHandler().GetFinishedSourceHandlers()->push_back(handler);
}
```

2. It sets the playback state of the `AudioScheduledSourceHandler` to `FINISHED_STATE`, allowing the `AudioScheduledSourceNode` to be deleted[4].

If a `suspend` is also scheduled at the same frame, we can then return to main thread and delete the `AudioScheduleSourceNode`. This is ok as the `AudioScheduledSourceHandler` is also being kept alive in `[active_source_handlers_]` when the `start` method of the source node is called[5], which is held in the `BaseAudioContext`.

```
void BaseAudioContext::NotifySourceNodeStartedProcessing(AudioNode* node) {
    DCHECK(!IsMainThread());
    GraphAutoLocker locker(this);

    GetDeferredTaskHandler().GetActiveSourceHandlers()->insert(&node->Handler());
    node->Handler().MakeConnection();
}
```

When the `BaseAudioContext` is resumed, it will call the `DeferredTaskHandler::BreakConnection` method in the `HandlePostRenderTasks` method[6] to finish off with the `AudioScheduleSourceNode`:

```
void DeferredTaskHandler::BreakConnections() {
    ...
    wtf_size_t size = finished_source_handlers_.size();
    if (size > 0) {
        for (auto* finished : finished_source_handlers_) {
            active_source_handlers_.erase(finished);    //<-- finished is now free'd
            finished->BreakConnectionWithLock();        //<-- UaF
        }
        finished_source_handlers_.clear();
    }
}
```

The problem, however, is that BreakConnections first erase the handler before using it in the next line. As the handler is now only kept alive by [active\_source\_handlers\_], this deletes the handler and causes UaF.

1.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/offline\\_audio\\_context.cc;l=413;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/offline_audio_context.cc;l=413;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
2.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/constant\\_source\\_node.cc;l=117;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/constant_source_node.cc;l=117;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
3.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/audio\\_scheduled\\_source\\_node.cc;l=242;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc;l=242;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
4.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/audio\\_scheduled\\_source\\_node.cc;l=243;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc;l=243;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
5.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/audio\\_scheduled\\_source\\_node.cc;l=199;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc;l=199;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
6.  
[https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third\\_party/blink/renderer/modules/webaudio/offline\\_audio\\_context.cc;l=426;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+71825939c432c440fa53ef4016372076e2c6114a:third_party/blink/renderer/modules/webaudio/offline_audio_context.cc;l=426;drc=b892cf58e162a8f66cd76d7472f129fe0fb6a7d1;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)

**VERSION**  
Chromium version: master branch build e577636  
Also tested on release google Chrome 80.3987.122  
Operating System: linux 18.04

**REPRODUCTION CASE**  
To reproduce the issue, run chromium with the expose-gc flag (this is just a convenient way to trigger gc and is not needed for the vulnerability)

`./out/asan/chrome --js-flags=-expose-gc --user-data-dir=/tmp`  
  
Then open the attached finished.html on localhost. It should produce an asan report like the one attached.

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

**asan**  
22.5 KB [View](#) [Download](#)

**finished.html**  
428 bytes [View](#) [Download](#)

Comment 1 by ClusterFuzz on Mon, Mar 2, 2020, 10:56 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=6197773337690112>.

Comment 2 by ClusterFuzz on Mon, Mar 2, 2020, 10:57 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5725722994868224>.

Comment 3 by ClusterFuzz on Mon, Mar 2, 2020, 10:57 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5634101410332672>.

Comment 4 by ClusterFuzz on Mon, Mar 2, 2020, 11:37 AM EST Project Member

Testcase 6197773337690112 failed to reproduce the crash. Please inspect the program output at <https://clusterfuzz.com/testcase?key=6197773337690112>.

Comment 5 by vakh@chromium.org on Mon, Mar 2, 2020, 1:43 PM EST Project Member

**Status:** Assigned (was: Unconfirmed)  
**Owner:** rtoy@chromium.org  
**Cc:** hongchan@chromium.org  
**Labels:** Security\_Severity-High Security\_Impact-Stable OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows  
**Components:** Blink>WebAudio  
  
Working on reproducing this locally.

Comment 6 by rtoy@chromium.org on Mon, Mar 2, 2020, 2:26 PM EST Project Member

**Status:** Started (was: Assigned)

Comment 7 by rtoy@chromium.org on Mon, Mar 2, 2020, 5:16 PM EST Project Member

The original test case reproduces for me with a local asan build. It looks like clusterfuzz can also reproduce this.

Thanks for the nice test case and summary of the problem. Fix on the way....

Comment 8 by bugdroid on Mon, Mar 2, 2020, 6:24 PM EST Project Member

The following revision refers to this bug:  
<https://chromium.googlesource.com/chromium/src.git/+3ac8883297e17ea27828bac2bcf39fa5e009f384>

commit 3ac8883297e17ea27828bac2bcf39fa5e009f384  
Author: Raymond Toy <rtoy@chromium.org>  
Date: Mon Mar 02 23:22:26 2020

Break connections before removing from active\_source\_handlers\_.

In DeferredTaskHandler::BreakConnections, we want to remove finished handlers and break the connection. when a finished handler is removed from active\_source\_handlers\_, it might be deleted, but we were still using that to create the connection. Instead, break the connection first and then remove it.

Manually ran test from the bug and it passes with this change. Without this, it failed right away.

[Bug-1067503](#)  
Change-Id: I3c9346a6842f412100d608876adb268befb80470

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2083436>  
Commit-Queue: Raymond Toy <[rtoy@chromium.org](mailto:rtoy@chromium.org)>  
Reviewed-by: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>  
Cr-Commit-Position: refs/heads/master@{#746142}

[modify] [https://crrev.com/3ac8883297e17ea27828bac2bcf39fa5e009f384/third\\_party/blink/renderer/modules/webaudio/deferred\\_task\\_handler.cc](https://crrev.com/3ac8883297e17ea27828bac2bcf39fa5e009f384/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc)

[Comment 9](#) by ClusterFuzz on Mon, Mar 2, 2020, 9:05 PM EST Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5634101410332672>

Fuzzer:

Job Type: linux\_asan\_chrome\_v8\_arm

Platform Id: linux

Crash Type: Heap-use-after-free READ 4

Crash Address: 0xf314c248

Crash State:

blink::AudioHandler::BreakConnectionWithLock

blink::DeferredTaskHandler::BreakConnections

blink::OfflineAudioContext::HandlePostRenderTasks

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: [https://clusterfuzz.com/revisions?job=linux\\_asan\\_chrome\\_v8\\_arm&range=635161:635170](https://clusterfuzz.com/revisions?job=linux_asan_chrome_v8_arm&range=635161:635170)

Reproducer Testcase: [https://clusterfuzz.com/download?testcase\\_id=5634101410332672](https://clusterfuzz.com/download?testcase_id=5634101410332672)

Additional requirements: Requires HTTP

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone <https://github.com/google/clusterfuzz> && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t <https://clusterfuzz.com/testcase-detail/5634101410332672> -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at <https://forms.gle/Yh3qCYFveHj6E5jz5> so we can improve.

[Comment 10](#) by ClusterFuzz on Mon, Mar 2, 2020, 9:08 PM EST Project Member

Detailed Report: <https://clusterfuzz.com/testcase?key=5725722994868224>

Fuzzer:

Job Type: linux\_asan\_chrome\_v8\_arm

Platform Id: linux

Crash Type: Heap-use-after-free READ 4

Crash Address: 0xf314c608

Crash State:

blink::AudioHandler::BreakConnectionWithLock

blink::DeferredTaskHandler::BreakConnections

blink::OfflineAudioContext::HandlePostRenderTasks

Sanitizer: address (ASAN)

Recommended Security Severity: High

Regressed: [https://clusterfuzz.com/revisions?job=linux\\_asan\\_chrome\\_v8\\_arm&range=635161:635170](https://clusterfuzz.com/revisions?job=linux_asan_chrome_v8_arm&range=635161:635170)

Reproducer Testcase: [https://clusterfuzz.com/download?testcase\\_id=5725722994868224](https://clusterfuzz.com/download?testcase_id=5725722994868224)

Additional requirements: Requires HTTP

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone <https://github.com/google/clusterfuzz> && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t <https://clusterfuzz.com/testcase-detail/5725722994868224> -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at <https://forms.gle/Yh3qCYFveHj6E5jz5> so we can improve.

[Comment 11](#) by [rtoy@chromium.org](mailto:rtoy@chromium.org) on Tue, Mar 3, 2020, 12:08 PM EST Project Member

I think it's fixed, but waiting for clusterfuzz to verify.

[Comment 12](#) by [sheriffbot](#) on Tue, Mar 3, 2020, 12:53 PM EST 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 13](#) by [sheriffbot](#) on Tue, Mar 3, 2020, 1:33 PM EST 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 14](#) by [rtoy@chromium.org](mailto:rtoy@chromium.org) on Tue, Mar 3, 2020, 7:04 PM EST Project Member

**Status:** Verified (was: Started)

Both <https://clusterfuzz.com/testcase-detail/5725722994868224> and <https://clusterfuzz.com/testcase-detail/5634101410332672> say the issue is fixed.

Closing as verified.

I'll let it bake for a day or two before requesting merges.

Comment 15 by rtoy@chromium.org on Wed, Mar 4, 2020, 10:44 AM EST Project Member

Labels: Merge-Request-81

Comment 16 by sheriffbot on Wed, Mar 4, 2020, 10:47 AM EST Project Member

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

This bug requires manual review. We are only 12 days from stable.

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](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), bindusuvama@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 17 by sheriffbot on Wed, Mar 4, 2020, 2:03 PM EST Project Member

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

Comment 18 by pbommana@google.com on Thu, Mar 5, 2020, 1:18 PM EST Project Member

Cc: adetaylor@chromium.org

+adetaylor@(Security TPM) for insights.

Comment 19 by pbommana@google.com on Thu, Mar 5, 2020, 1:18 PM EST Project Member

Cc: pbomm...@chromium.org

Comment 20 by adetaylor@chromium.org on Thu, Mar 5, 2020, 1:58 PM EST Project Member

Labels: -Merge-Review-81 Merge-Approved-81

I am in favor of merging to M81, yes. This looks like a simple and low-risk fix. I'm going to approve merge to M81 (branch 4044) even before we get the answers to #c16, but please don't merge if there are any concerns I haven't spotted. Also, please check for unexpected canary trouble before merging.

Comment 21 by rtoy@chromium.org on Thu, Mar 5, 2020, 2:16 PM EST Project Member

crash.corp doesn't seem to show any crashes in M81 or later, but they weren't super-common to begin with. Clusterfuzz has verified that the UaF is gone. (Don't know why the two test cases didn't report this was fixed, but the webpage says it is.)

Comment 22 by bugdroid on Thu, Mar 5, 2020, 4:07 PM EST Project Member

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+765cc3c01c8f68317cdfd610981f1182404f718e>

commit 765cc3c01c8f68317cdfd610981f1182404f718e

Author: Raymond Toy <rtoy@chromium.org>

Date: Thu Mar 05 21:06:37 2020

Break connections before removing from active\_source\_handlers\_.

In DeferredTaskHandler::BreakConnections, we want to remove finished handlers and break the connection. when a finished handler is removed from active\_source\_handlers\_, it might be deleted, but we were still using that to create the connection. Instead, break the connection first and then remove it.

Manually ran test from the bug and it passes with this change. Without this, it failed right away.

(cherry picked from commit 3ac8883297e17ea27828bac2bcf39fa5e009f384)

~~Bug=4067509~~

Change-Id: I3c9346a6842f412100d608876adb268befb80470

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2083436>

Commit-Queue: Raymond Toy <rtoy@chromium.org>

Reviewed-by: Hongchan Choi <hongchan@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#746142}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2090296>

Reviewed-by: Raymond Toy <rtoy@chromium.org>

Cr-Commit-Position: refs/branch-heads/4044@{#650}

Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] [https://crrev.com/765cc3c01c8f68317cdfd610981f1182404f718e/third\\_party/blink/renderer/modules/webaudio/deferred\\_task\\_handler.cc](https://crrev.com/765cc3c01c8f68317cdfd610981f1182404f718e/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc)

Comment 23 by rtoy@chromium.org on Fri, Mar 6, 2020, 3:15 PM EST Project Member

Given that the M81 branch cut is very soon, I'm going to assume that a merge to M80 is not warranted.

Comment 24 by adetaylor@chromium.org on Fri, Mar 6, 2020, 3:33 PM EST Project Member

Agreed.

Comment 25 by mmoroz@google.com on Tue, Mar 10, 2020, 1:04 PM EDT Project Member

Labels: VulnerabilityAnalysis-Requested

rtoy@, thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: <https://forms.gle/VWKDUv9a8GXCCRWm7>

Comment 26 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT Project Member

Labels: Release-0-M81

Comment 27 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:30 PM EDT Project Member

Labels: CVE-2020-6428 CVE\_description-missing

Comment 28 by bugdroid on Mon, Mar 16, 2020, 1:59 AM EDT Project Member

**Labels:** merge-merged-3987\_137

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+a5f00911c397b8b3d9234dd5f366d6ef1024e51d>

commit [a5f00911c397b8b3d9234dd5f366d6ef1024e51d](#)

Author: Raymond Toy <[rtoy@chromium.org](mailto:rtoy@chromium.org)>

Date: Mon Mar 16 05:58:01 2020

Break connections before removing from active\_source\_handlers\_.

In DeferredTaskHandler::BreakConnections, we want to remove finished handlers and break the connection. when a finished handler is removed from active\_source\_handlers\_, it might be deleted, but we were still using that to create the connection. Instead, break the connection first and then remove it.

Manually ran test from the bug and it passes with this change. Without this, it failed right away.

(cherry picked from commit [3ac8883297e17ea27828bac2bcf39fa5e009f384](#))

~~[Bug-1057593](#)~~

Change-Id: [I3c9346a6842f412100d608876adb268befb80470](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2083436>

Commit-Queue: Raymond Toy <[rtoy@chromium.org](mailto:rtoy@chromium.org)>

Reviewed-by: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Cr-Original-Commit-Position: refs/heads/master@{#746142}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2104827>

Reviewed-by: Krishna Govind <[govind@chromium.org](mailto:govind@chromium.org)>

Reviewed-by: Prudhvi Kumar Bommana <[pbommana@google.com](mailto:pbommana@google.com)>

Cr-Commit-Position: refs/branch-heads/3987\_137@{#6}

Cr-Branched-From: [55c16ce255e7a7feca588abeb4f082026b35e1ef](#)-refs/branch-heads/3987@{#989}

Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#722274}

[modify] [https://crrev.com/a5f00911c397b8b3d9234dd5f366d6ef1024e51d/third\\_party/blink/renderer/modules/webaudio/deferred\\_task\\_handler.cc](https://crrev.com/a5f00911c397b8b3d9234dd5f366d6ef1024e51d/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc)

[Comment 29](#) by [rtoy@chromium.org](mailto:rtoy@chromium.org) on Mon, Mar 16, 2020, 1:51 PM EDT Project Member

If you are going to merge this bug fix to M80, you should also probably get the fix in [issue-1050686](#). It's closely related, and this fix didn't fix all the cases. [issue-1050686](#) has a better fix.

[Comment 30](#) by [gov...@chromium.org](mailto:gov...@chromium.org) on Mon, Mar 16, 2020, 8:42 PM EDT Project Member

**Labels:** Merge-Approved-80

Approving merge to M80 branch 3987, please merge ASAP. Thank you.

[Comment 31](#) by [bugdroid](#) on Mon, Mar 16, 2020, 8:56 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/+ee14ad040d6acd683eaa1bbb5acb8e979d1b9560>

commit [ee14ad040d6acd683eaa1bbb5acb8e979d1b9560](#)

Author: Raymond Toy <[rtoy@chromium.org](mailto:rtoy@chromium.org)>

Date: Tue Mar 17 00:54:20 2020

Break connections before removing from active\_source\_handlers\_.

In DeferredTaskHandler::BreakConnections, we want to remove finished handlers and break the connection. when a finished handler is removed from active\_source\_handlers\_, it might be deleted, but we were still using that to create the connection. Instead, break the connection first and then remove it.

Manually ran test from the bug and it passes with this change. Without this, it failed right away.

~~[Bug-1057593](#)~~

Change-Id: [I3c9346a6842f412100d608876adb268befb80470](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2083436>

Commit-Queue: Raymond Toy <[rtoy@chromium.org](mailto:rtoy@chromium.org)>

Reviewed-by: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#746142}

(cherry picked from commit [3ac8883297e17ea27828bac2bcf39fa5e009f384](#))

TBR=[rtoy@chromium.org](mailto:rtoy@chromium.org)

Change-Id: [I3c9346a6842f412100d608876adb268befb80470](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2106771>

Reviewed-by: Krishna Govind <[govind@chromium.org](mailto:govind@chromium.org)>

Commit-Queue: Krishna Govind <[govind@chromium.org](mailto:govind@chromium.org)>

Cr-Commit-Position: refs/branch-heads/3987@{#1007}

Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](#)-refs/heads/master@{#722274}

[modify] [https://crrev.com/ee14ad040d6acd683eaa1bbb5acb8e979d1b9560/third\\_party/blink/renderer/modules/webaudio/deferred\\_task\\_handler.cc](https://crrev.com/ee14ad040d6acd683eaa1bbb5acb8e979d1b9560/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc)

[Comment 32](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Tue, Mar 17, 2020, 11:17 AM EDT Project Member

**Labels:** -Release-0-M81 Release-5-M80

[Comment 33](#) by [gov...@chromium.org](mailto:gov...@chromium.org) on Tue, Mar 17, 2020, 4:33 PM EDT Project Member

**Cc:** [prashanthpola@chromium.org](mailto:prashanthpola@chromium.org)

[Comment 34](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Thu, Mar 19, 2020, 6:30 PM EDT Project Member

**Labels:** -CVE\_description-missing CVE\_description-submitted

[Comment 35](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Mar 25, 2020, 3:31 PM EDT Project Member

**Cc:** [achuith@chromium.org](mailto:achuith@chromium.org)

[Comment 36](#) by [sheriffbot](#) on Wed, Jun 10, 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