




☆ Starred by 1 user

Owner:	 hongchan@chromium.org OOO (12.15-1.8)
CC:	adetaylor@chromium.org  prashanthpola@chromium.org  rtoy@chromium.org achuith@chromium.org
Status:	Verified (Closed)
Components:	Blink>WebAudio
Modified:	Jun 4, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review  
Security\_Impact-Stable  
Security\_Severity-High  
allpublic  
CVE\_description-submitted  
M-81  
merge-merged-3987  
merge-merged-80  
merge-merged-4044  
merge-merged-81  
CVE-2020-6427  
merge-merged-3987\_137  
Release-5-M80

Issue 1055788: UaP in IIRFilterHandler::Process  
Reported by m...@semmlie.com on Tue, Feb 25, 2020, 10:33 AM EST

🔗 Code

VULNERABILITY DETAILS

In the IIRFilterHandler::Process method, if an infinite output is encountered, the method IIRFilterHandler::NotifyBadState method will be posted to the main thread[1]:

```
if (!HasNonFiniteOutput()) {
    did_warn_bad_filter_state_ = true;

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

The method IIRFilterHandler::NotifyBadState first checks for Context and then call Context()->GetExecutionContext()[2].

```
void IIRFilterHandler::NotifyBadState() const {
    DCHECK(IsMainThread());
    if (!Context() || !Context()->GetExecutionContext())
        return;
```

However, as Context is an UntracedMember[3], it is possible to remove it while the IIRFilterHandler::NotifyBadState method is waiting in the main queue. This then causes UaP and subsequently UaF in NotifyBadState.

The BiquadFilterHandler also has an identical routine, so it probably is also vulnerable to this issue [4].

1. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc;l=108;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/iir_filter_node.cc;l=108;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
2. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc;l=117;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/iir_filter_node.cc;l=117;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
3. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/audio\\_node.h;drc=5cc67ce9c0e922a742dc0064ad38c4f8f9668aa9;bpv=1;bpt=1;l=291?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/audio_node.h;drc=5cc67ce9c0e922a742dc0064ad38c4f8f9668aa9;bpv=1;bpt=1;l=291?originalUrl=https:%2F%2Fcs.chromium.org%2F)
4. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.cc;l=88;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/biquad_filter_node.cc;l=88;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)

VERSION  
Chrome version: master branch build 8f57323, release build.  
Operating System: Ubuntu 18.04

REPRODUCTION CASE

Include the attached files badstate1.html, badstate2.html and sample.mp3 in the same directory and then serve it on local host. Then open badstate2.html with a Chromium asan build.

```
/out/asan/chrome --js-flags=-expose-gc --user-data-dir=/tmp
```

I am able to reproduce the issue on commit 8f57323 in the master branch in less then a minute most of the time. (The page will keep reloading until it succeeded) However, I appreciate that the issue is sensitive to timing and may depend somewhat on the machine that is tested (mostly the timeout time in badstate2.html:30 and the sleep time in badstate1.html:53 may need tweaking, the idea is to arrange the timeout so that the removal of the iframe happens sometime after the processing started but before NotifyBadState got posted), so please let me know if you have problem reproducing it. If successful, it should produce the attached asan log.

Thank you very much for your help and please let me know if there is anything I can help. Thanks.

CREDIT INFORMATION

Reporter credit: Man Yue Mo of GitHub Security Lab

- badstate1.html  
1.8 KB View Download
- badstate2.html  
722 bytes View Download
- sample.mp3  
39.7 KB Download
- asan  
4.6 KB View Download

Comment 1 by vakh@chromium.org on Tue, Feb 25, 2020, 2:17 PM EST Project Member

Owner: rtoy@chromium.org  
Cc: hongchan@chromium.org  
Components: Blink>WebAudio

Thanks for the report.  
I'm still working on reproducing it, but in the meantime adding the OWNERS and the component.

Comment 2 by vakh@chromium.org on Tue, Feb 25, 2020, 2:23 PM EST Project Member

Labels: Security\_Severity-High

Comment 3 by sheriffbot on Tue, Feb 25, 2020, 2:39 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 4 by hongchan@chromium.org on Tue, Feb 25, 2020, 3:30 PM EST Project Member

So the culprit here is Context()->GetExecutionContext(). We can simply bail out when the Context()->IsContextCleared() is true.

```
---
#0 0x7f50ef43794c in GetRaw J.J.J./third_party/blink/renderer/platform/heap/member.h:232:44
#1 0x7f50ef43794c in operator blink::ContextLifecycleNotifier * J.J.J./third_party/blink/renderer/platform/heap/member.h:184:32
#2 0x7f50ef43794c in GetContextLifecycleNotifier J.J.J./third_party/blink/renderer/platform/context_lifecycle_observer.h:24:12
#3 0x7f50ef43794c in blink::ExecutionContextLifecycleObserver::GetExecutionContext() const
J.J.J./third_party/blink/renderer/core/execution_context/execution_context_lifecycle_observer.cc:62:41
#4 0x7f50e477a07b in blink::UIEventHandler::NotifyBadState() const J.J.J./third_party/blink/renderer/modules/webaudio/iir_filter_node.cc:117:33
#5 0x7f51114f6dc2 in Run J.J.J./base/callback.h:98:12
#6 0x7f51114f6dc2 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) J.J.J./base/task/common/task_annotator.cc:142:3
(omitted)
---
```

Notes:  
- This is reproduced on <https://chromiumdash.appspot.com/commit/8f57323a704780f0aa5557cbe7a633420642cc1>  
- The bug filed after the self-referencing patch landed (<https://chromium.googlesource.com/chromium/src/+85f708fa7ab898c7ae678c0b8a270105be6bbb4e>)

Comment 5 by hongchan@chromium.org on Tue, Feb 25, 2020, 4:44 PM EST Project Member

Labels: OS-Linux

Couldn't reproduce on MacOS 82.0.4070.0.

Comment 6 by hongchan@chromium.org on Tue, Feb 25, 2020, 4:44 PM EST Project Member

Labels: Pri-1

Comment 7 by vakh@chromium.org on Tue, Feb 25, 2020, 5:50 PM EST Project Member

Labels: Security\_Impact-Head

Comment 8 by m...@semml.com on Wed, Feb 26, 2020, 5:38 AM EST

Thanks for looking into this.

The issue is not so much about the GetExecutionContext() method but rather that the UntracedMember context\_ has already been collected by the time NotifyBadState is called. So checking Context()->IsContextCleared() is not going to help because it is also calling a method in context\_ which, if the bug is successfully exploited, will be in controlled of the attacker.

The problem is that the current mechanism for UaF prevention has some invalid assumptions:  
1. As an AudioHandler is stored as a scope\_refptr in the corresponding AudioNode [1], it cannot be destroyed when AudioNode is alive. Since context is also held as a Member in AudioNode [2], AudioNode is responsible to keep context alive while AudioHandler is alive. However, when AudioNode is destroyed, one of the two things may happen:  
a. If a graph is being pulled while AudioNode is being collected, then it will transfer ownership of the AudioHandler to the deferred\_task\_handler and store it there as a rendering\_orphan\_handler. [3]

```
if (context()->IsPullingAudioGraph()) {
  context()->GetDeferredTaskHandler().AddRenderingOrphanHandler(
    std::move(handler_));
}
```

When context\_ is destroyed, it will then clear itself up from the handlers in rendering\_orphan\_handlers\_ by first calling DeferredTaskHandler::ContextWillBeDestroyed [4], which then clears context\_ in the handlers in rendering\_orphan\_handlers\_ to prevent UaF[5]. This relies on the assumption that rendering\_orphan\_handlers\_ does not change between the removal of the AudioNode and the destruction of the BaseAudioContext.

b. If a graph is not being pulled, then ownership transferred will not take place and AudioNode will be destroyed, after which, context\_ may also be destroyed. If AudioNode is the sole owner of the AudioHandler, then AudioHandler will also be destroyed at this point.

The problem is that either of these assumptions may not be valid.

For case a, it is possible to have the following event sequence:

NotifyBadState posted to main thread -> AudioNode::Dispose (pulling graph, AudioHandler now held in rendering\_orphan\_handlers\_) -> BaseAudioContext::Uninitialize (will call ClearHandlersToBeDeleted to clear rendering\_orphan\_handlers\_) -> ~BaseAudioContext (will not clear context\_ in the AudioHandler as it is no longer in rendering\_orphan\_handlers\_) -> NotifyBadState (UaP/UaF)

The reproduction case in this ticket uses this flaw and tries to place an Uninitialize task in between AudioNode::Dispose and ~OfflineAudioContext to trigger this bug.

For case b, the following sequence will also trigger the bug:

NotifyBadState posted to main thread (as a scoped\_refptr) -> Graph pulling disabled -> AudioNode::Dispose (no ownership transfer) -> ~AudioContext (No one holding reference to it) -> NotifyBadState (UaP/UaF)

The problem here is that, when AudioNode gets destroyed, the posted NotifyBadState task still holds a reference to AudioHandler, but there is nothing there to keep AudioContext alive anymore, but NotifyBadState still lives in the task, which then uses the now destroyed AudioContext. This seems to be only possible with AudioContext and I have not been able to trigger the bug using this path. I suspect this is due to the self-referencing patch.

As for fixing this issue, there are different ways to do so.

1. By closing the loopholes in the clean up logic. For case a, make sure that every time rendering\_orphan\_handlers\_ changes, ClearContext of the handlers is called. This seems to happen only in ClearHandlersToBeDeleted, so the clean up logic inside ~BaseAudioContext can probably be merged into ClearHandlersToBeDeleted. For case b, probably can call ClearContext of the handler in AudioNode::Dispose if the ownership is not transferred. This may have more risk of affecting the code but should be safer and can prevent similar problems.

2. To fix the current issue only, changing the scoped\_refptr to weak ptr when posting NotifyBadState[6] should invalidate the handler once rendering\_orphan\_handlers\_ is cleared and NotifyBadState will not trigger. This should not affect the behaviour of the code other than fixing the current issue.

I'm curious about why the self-referencing patch would change the behaviour of the test case, as the patch only changes functionality in AudioContext and the test case only uses OfflineAudioContext. I'll do some investigation with the 80.0.3987.122 build and see what's going on there.

1. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/audio\\_node.h;l=401;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/audio_node.h;l=401;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
2. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/audio\\_node.h;l=396;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/audio_node.h;l=396;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
3. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/audio\\_node.cc;l=618;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/audio_node.cc;l=618;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
4. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/base\\_audio\\_context.cc;l=112;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/base_audio_context.cc;l=112;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
5. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/deferred\\_task\\_handler.cc;l=297;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc;l=297;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)
6. [https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc;l=109;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F](https://source.chromium.org/chromium/chromium/src/+b4c8e1370db91786c807e01ca6d56a88b4054070:third_party/blink/renderer/modules/webaudio/iir_filter_node.cc;l=109;bpv=1;bp=1?originalUrl=https:%2F%2Fcs.chromium.org%2F)

Comment 9 by [vakh@chromium.org](mailto:vakh@chromium.org) on Wed, Feb 26, 2020, 11:15 AM EST Project Member

Labels: M-82

Comment 10 by [hongchan@chromium.org](mailto:hongchan@chromium.org) on Wed, Feb 26, 2020, 12:39 PM EST Project Member

Thanks for the detailed analysis. :)

I also just confirmed the reproduction on Linux.

The cleanup logic is the most fragile area in the WebAudio code. It has been built over years of patches, and it needs clean up/refactoring soon. For this issue, I took a minimal approach so we can do the merge to other release branches.

NVM on the self-referencing patch. I naively assumed the repro uses AudioContext. In short, it solves the issue in an opposite way by making the AudioContext alive until the resources are explicitly cleared.

Comment 11 by [sheriffbot](mailto:sheriffbot) on Wed, Feb 26, 2020, 1:22 PM EST Project Member

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 12 by [bugdroid](mailto:bugdroid) on Wed, Feb 26, 2020, 11:29 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+2cd0af7ea20547c2471483ef2233f3b068db93c3>

commit [2cd0af7ea20547c2471483ef2233f3b068db93c3](https://chromium.googlesource.com/chromium/src.git/+2cd0af7ea20547c2471483ef2233f3b068db93c3)

Author: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Date: Thu Feb 27 04:24:46 2020

Use WeakPtr for cross-thread posting

{IIR,Biquad}FilterNodes check the state of the filter and notify the main thread when it goes bad. In this process, the associated context can be collected when a posted task is performed sometime later in the task runner's queue.

By using WeakPtr, the task runner will not perform a scheduled task in the queue when the target object is invalid anymore.

Test: Locally confirmed that the repro case does not crash after 30 min.

[Bug-1056708](#)

Change-Id: [Icdb3a7378d0345936b5b50e12ec2b187e58a611c](https://chromium-review.googlesource.com/c/chromium/src/+2074807)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2074807>

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

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

Reviewed-by: Kentaro Hara <[haraken@chromium.org](mailto:haraken@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#744936}

[modify] [https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.cc](https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third_party/blink/renderer/modules/webaudio/biquad_filter_node.cc)

[modify] [https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.h](https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third_party/blink/renderer/modules/webaudio/biquad_filter_node.h)

[modify] [https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc](https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third_party/blink/renderer/modules/webaudio/iir_filter_node.cc)

[modify] [https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.h](https://crrev.com/2cd0af7ea20547c2471483ef2233f3b068db93c3/third_party/blink/renderer/modules/webaudio/iir_filter_node.h)

Comment 13 by [hongchan@chromium.org](#) on Wed, Feb 26, 2020, 11:29 PM EST Project Member

**Status:** Started (was: Assigned)  
**Owner:** [hongchan@chromium.org](#)  
**Cc:** [-hongchan@chromium.org](#) [rtoy@chromium.org](#)

Comment 14 by [hongchan@chromium.org](#) on Wed, Feb 26, 2020, 11:29 PM EST Project Member

**Status:** Fixed (was: Started)

Comment 15 by [hongchan@chromium.org](#) on Wed, Feb 26, 2020, 11:31 PM EST Project Member

**Labels:** Needs-Feedback

mmo@

The fix is landed and it would be great if you can verify it.

Comment 16 by [m...@semml.com](#) on Thu, Feb 27, 2020, 4:45 AM EST

Thanks for the fix.

The fix looks good and I've verified that the test case does not crash anymore and that the fix correctly prevents NotifyBadState from being called after `|rendering_orphan_handlers_|` is cleared, which prevented the issue.

I've also verified that the issue reproduces on an asan build of 80.0.3987.122 (current release) on linux. Would you be able to verify it and perhaps update the `Security_Impact` as appropriate? Thanks.

Also, while the patch fixes the current issue and introduces minimal risk for the release. I'd suggest also to create a CL with the attached patch to address the wider issue, and release it after you have enough time to test it and are happy with it. This patch makes sure that `|context_|` is cleared before `|rendering_orphan_handlers_|` is cleared. It may alter the behaviour in the case where a handler is put in the `|rendering_orphan_handlers_|` collection, and then the execution context is destroyed, (which clears this collection) but for some reason the `(Offline)AudioContext` is not destroyed (e.g. held in another context). In that case, the handler will lose the `(Offline)AudioContext` but then the `(Offline)AudioContext` should not be rendering anymore in that case, so the risk shouldn't be that high.

**cleanup.patch**  
1.2 KB [View](#) [Download](#)

Comment 17 by [sheriffbot](#) on Thu, Feb 27, 2020, 2:05 PM EST Project Member

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

Comment 18 by [hongchan@chromium.org](#) on Thu, Feb 27, 2020, 2:51 PM EST Project Member

**Status:** Verified (was: Fixed)

Comment 19 by [hongchan@chromium.org](#) on Thu, Feb 27, 2020, 2:57 PM EST Project Member

Thanks for the verification! I'll let security folks handle the label change.

Also I really appreciate the suggestion, but I would rather handle it with a new issue. If you have a repro case that demonstrates the exploit, I can create the issue and start working on it.

Comment 20 by [hongchan@chromium.org](#) on Thu, Feb 27, 2020, 2:58 PM EST Project Member

**Cc:** [adetaylor@chromium.org](#)  
**Labels:** -Needs-Feedback

cc-ing [adetaylor@](#) for the potential merge to M81, M80.

Comment 21 by [adetaylor@chromium.org](#) on Thu, Feb 27, 2020, 6:05 PM EST Project Member

**Labels:** -Security\_Impact-Head Security\_Impact-Stable

Per [#c16](#) updating `Security_Impact`, which will cause Sheriffbot to add lots of merge request labels tomorrow morning. I don't think we'll quite have enough Canary time to get this into the next stable refresh, so it's likely to be the one after.

Comment 22 by [adetaylor@google.com](#) on Mon, Mar 9, 2020, 2:34 PM EDT Project Member

**Labels:** -ReleaseBlock-Stable -M-82 M-81 Merge-Request-81

The manual targeting at M-82 prevented the rash of merge request labels, so based on [#c16](#) retargeting and adding merge request to 81.

Comment 23 by [sheriffbot](#) on Mon, Mar 9, 2020, 2:36 PM EDT Project Member

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

This bug requires manual review: We are only 7 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 24 by [hongchan@chromium.org](#) on Mon, Mar 9, 2020, 2:55 PM EDT Project Member

1. This is a small change and I did not see anything worrisome from Canary.
2. <https://chromium-review.googlesource.com/c/chromium/src/+2074807>
3. Yes.
4. This is a P1 stable release blocker.
5. No.
6. N/A

Comment 25 by [adetaylor@chromium.org](#) on Mon, Mar 9, 2020, 4:20 PM EDT Project Member

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

Thanks. Please merge to M81, branch 4044.

Comment 26 by [bugdroid](#) on Mon, Mar 9, 2020, 6:42 PM EDT 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/+9679a2038353cfb257af78d66b24db3a8f416441>

commit [9679a2038353cfb257af78d66b24db3a8f416441](#)

Author: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Date: Mon Mar 09 22:41:51 2020

Use WeakPtr for cross-thread posting

{IIR,Biquad}FilterNodes check the state of the filter and notify the main thread when it goes bad. In this process, the associated context can be collected when a posted task is performed sometime later in the task runner's queue.

By using WeakPtr, the task runner will not perform a scheduled task in the queue when the target object is invalid anymore.

(cherry picked from commit [2cd0af7ea20547c2471483ef2233f3b068db93c3](#))

Test: Locally confirmed that the repro case does not crash after 30 min.

~~Bug-1056700~~

Change-Id: [Icdb3a7378d0345936b5b50e12ec2b187e58a611c](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2074807>

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

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

Reviewed-by: Kentaro Hara <[haraken@chromium.org](mailto:haraken@chromium.org)>

Cr-Original-Commit-Position: refs/heads/master@{#744936}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2095148>

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

Cr-Commit-Position: refs/branch-heads/4044@{#726}

Cr-Branched-From: [a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}](#)

[modify] [https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.cc](https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third_party/blink/renderer/modules/webaudio/biquad_filter_node.cc)

[modify] [https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.h](https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third_party/blink/renderer/modules/webaudio/biquad_filter_node.h)

[modify] [https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc](https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third_party/blink/renderer/modules/webaudio/iir_filter_node.cc)

[modify] [https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.h](https://crrev.com/9679a2038353cfb257af78d66b24db3a8f416441/third_party/blink/renderer/modules/webaudio/iir_filter_node.h)

**Comment 27** by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, Mar 13, 2020, 1:44 PM EDT Project Member

**Labels:** Release-0-M81

**Comment 28** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Fri, Mar 13, 2020, 2:30 PM EDT Project Member

**Labels:** CVE-2020-6427 CVE\_description-missing

**Comment 29** by [bugdroid](mailto:bugdroid) on Mon, Mar 16, 2020, 2:08 AM EDT Project Member

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+a937edde33870370783e99f5cc2e261f40be2bdb>

commit [a937edde33870370783e99f5cc2e261f40be2bdb](#)

Author: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Date: Mon Mar 16 06:07:19 2020

Use WeakPtr for cross-thread posting

{IIR,Biquad}FilterNodes check the state of the filter and notify the main thread when it goes bad. In this process, the associated context can be collected when a posted task is performed sometime later in the task runner's queue.

By using WeakPtr, the task runner will not perform a scheduled task in the queue when the target object is invalid anymore.

(cherry picked from commit [2cd0af7ea20547c2471483ef2233f3b068db93c3](#))

Test: Locally confirmed that the repro case does not crash after 30 min.

~~Bug-1056700~~

Change-Id: [Icdb3a7378d0345936b5b50e12ec2b187e58a611c](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2074807>

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

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

Reviewed-by: Kentaro Hara <[haraken@chromium.org](mailto:haraken@chromium.org)>

Cr-Original-Commit-Position: refs/heads/master@{#744936}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2104664>

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@{#8}

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

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

[modify] [https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.cc](https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third_party/blink/renderer/modules/webaudio/biquad_filter_node.cc)

[modify] [https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.h](https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third_party/blink/renderer/modules/webaudio/biquad_filter_node.h)

[modify] [https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc](https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third_party/blink/renderer/modules/webaudio/iir_filter_node.cc)

[modify] [https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.h](https://crrev.com/a937edde33870370783e99f5cc2e261f40be2bdb/third_party/blink/renderer/modules/webaudio/iir_filter_node.h)

**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](mailto:bugdroid) on Mon, Mar 16, 2020, 9:02 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/+4df3de1000eae398f53220d10b964cd01640ca9>

commit [4df3de1000eae398f53220d10b964cd01640ca9](#)

Author: Hongchan Choi <[hongchan@chromium.org](mailto:hongchan@chromium.org)>

Date: Tue Mar 17 01:01:18 2020

Use WeakPtr for cross-thread posting

{IIR,Biquad}FilterNodes check the state of the filter and notify the main thread when it goes bad. In this process, the associated context

can be collected when a posted task is performed sometime later in the task runner's queue.

By using WeakPtr, the task runner will not perform a scheduled task in the queue when the target object is invalid anymore.

(cherry picked from commit [2cd0af7ea20547c2471483ef2233f3b068db93c3](#))

(cherry picked from commit [a937edde33870370783e99f5cc2e261f40be2bdb](#))

Test: Locally confirmed that the repro case does not crash after 30 min.

~~bug-4056746~~

Change-Id: Icd3a7378d0345936b5b50e12ec2b187e58a611c

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2074807>

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

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

Reviewed-by: Kentaro Hara <[haraken@chromium.org](mailto:haraken@chromium.org)>

Cr-Original-Original-Commit-Position: refs/heads/master@{#744936}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2104664>

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

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

Cr-Original-Commit-Position: refs/branch-heads/3987\_137@{#8}

Cr-Original-Branched-From: 55c16ce255e7a7feca588abeb4f082026b35e1ef-refs/branch-heads/3987@{#989}

Cr-Original-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2106745>

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

Cr-Commit-Position: refs/branch-heads/3987@{#1009}

Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] [https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.cc](https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third_party/blink/renderer/modules/webaudio/biquad_filter_node.cc)

[modify] [https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third\\_party/blink/renderer/modules/webaudio/biquad\\_filter\\_node.h](https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third_party/blink/renderer/modules/webaudio/biquad_filter_node.h)

[modify] [https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.cc](https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third_party/blink/renderer/modules/webaudio/iir_filter_node.cc)

[modify] [https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third\\_party/blink/renderer/modules/webaudio/iir\\_filter\\_node.h](https://crrev.com/4df3de1000eae398f53220d10b964cd01640ca9/third_party/blink/renderer/modules/webaudio/iir_filter_node.h)

[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

[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

[Comment 36](#) by [m...@semmlie.com](mailto:m...@semmlie.com) on Tue, Apr 7, 2020, 4:51 AM EDT

adetaylor@ Sorry to bother you about this, but it looks like the credit information in the release notes has the incorrect affiliation, instead of Semmlie Security Research Team, the affiliation should be GitHub Security Lab. (This should be my affiliation from now on) There's no rush, but do you mind updating the affiliation for this and the other tickets when it's convenient for you? Thank you very much for your help.

[Comment 37](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Tue, Apr 7, 2020, 11:05 AM EDT Project Member

OK, sorry for not spotting the change. Hopefully all the notes are correctly updated now - let me know if you spot something that still isn't right. Thanks again for all the reports!

[Comment 38](#) by [m...@semmlie.com](mailto:m...@semmlie.com) on Tue, Apr 7, 2020, 11:17 AM EDT

No worries, thank you very much for your help. Everything looks correct now, thanks.

[Comment 39](#) by [sheriffbot](mailto:sheriffbot) on Thu, Jun 4, 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