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:	Fixed *(Closed)*
Components:	Blink>WebAudio
Modified:	Jun 10, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
M-80
Security_Severity-High
allpublic
CVE_description-submitted
Target-80
Merge-Rejected-80
merge-merged-3987
merge-merged-80
merge-merged-4044
merge-merged-81
CVE-2020-6429
merge-merged-3987_137
Release-5-M80

Issue 1057627: UaP in AudioScheduledSourceHandler::NotifyEnded

Reported by m...@semmle.com on Mon, Mar 2, 2020, 9:53 AM EST

Code

VULNERABILITY DETAILS

This issue is similar to 1055788, in that an AudioHandler is being posted to a task queue as a scoped_refptr and the context_ UntracedMember is destroyed while it is waiting in the task queue.

The AudioScheduledSourceHandler::Finish method is called in the pre-rendering stage when DeferredTaskHandler::HandlePreRenderTask is called and a stop is scheduled. (OfflineAudioContext::HandlePreRenderTasks -> HandleStoppableSourceNodes -> AudioScheduledSourceHandler::HandleStoppableSourceNode -> AudioScheduledSourceHandler::Finish)

This method posts a task to the main thread, wrapping the handler as a scoped_refptr:

```
void AudioScheduledSourceHandler::Finish() {
  FinishWithoutOnEnded();

  PostCrossThreadTask(
      *task_runner_, FROM_HERE,
      CrossThreadBindOnce(&AudioScheduledSourceHandler::NotifyEnded,
                          WrapRefCounted(this)));
}
```

The AudioScheduledSourceHandler::NotifyEnded method then calls GetExecutionContext. However, it is possible for |context_| to be destroyed while NotifyEnded is waiting in the queue. This will cause UaP/UaF when Context()->GetExecutionContext() is called in NotifyEnded.

```
void AudioScheduledSourceHandler::NotifyEnded() {
  DCHECK(IsMainThread());
  if (!Context() || !Context()->GetExecutionContext())
    return;
  if (GetNode())
    GetNode()->DispatchEvent(*Event::Create(event_type_names::kEnded));
}
```

A more detailed analysis can be found in ticket 1055788.

VERSION

Chrome version: master branch build e577636, release build 80.3987.122
Operating System: Ubuntu 18.04

REPRODUCTION CASE

Include the attached files stop1.html and stop2.html in the same directory and then serve it on localhost. Launch asan build chrome and then open stop2.html

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

This reproduces fairly reliably on my machine and normally crash after the first reload for both the master and release build. However, I appreciate that this issue is sensitive to timing and maybe somewhat machine dependent, so please let me know if you yhave 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 that I can help. Thanks.

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

stop1.html
582 bytes View Download

stop2.html
616 bytes View Download

asan
4.4 KB View Download

Comment 1 by vakh@chromium.org on Mon, Mar 2, 2020, 11:09 AM EST Project Member

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

Thanks for the report.
Adding platforms based on BUILD.gn, which may not be accurate.

Comment 2 by rtoy@chromium.org on Mon, Mar 2, 2020, 11:51 AM EST Project Member

Yeah, looks pretty similar to ~~issue 1055789~~ and can probably be solved the same way.

Comment 3 by sheriffbot on Mon, Mar 2, 2020, 12:51 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 4 by sheriffbot on Mon, Mar 2, 2020, 1:32 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 5 by hongchan@chromium.org on Mon, Mar 2, 2020, 2:13 PM EST Project Member

Status: Started (was: Assigned)

mmo@ Thanks for the report!

Comment 6 by hongchan@chromium.org on Mon, Mar 2, 2020, 2:43 PM EST Project Member

Labels: -OS-Mac

I guess it's the same way because I can't reproduce on MacOS (Version 82.0.4076.0).

Comment 7 by hongchan@chromium.org on Tue, Mar 3, 2020, 11:36 AM EST Project Member

Reproducible on Linux and also confirmed the patch in the works is effective.

Comment 8 by bugdroid on Tue, Mar 3, 2020, 7:46 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/913247c378d54e0378ffd09524e0aa7503035fc4

commit 913247c378d54e0378ffd09524e0aa7503035fc4
Author: Hongchan Choi <hongchan@chromium.org>
Date: Wed Mar 04 00:45:41 2020

Use SupportsWeakPtr for messaging from rendering thread to main thread

In cross-thread messaging, the associated execution context can be
already gone 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.

Test: Locally confirmed that the repro does not crash.
~~Bug: 1057627~~
Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/heads/master@{#746613}

[modify] https://crrev.com/913247c378d54e0378ffd09524e0aa7503035fc4/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/913247c378d54e0378ffd09524e0aa7503035fc4/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 9 by hongchan@chromium.org on Wed, Mar 4, 2020, 11:32 AM EST Project Member

Status: Fixed (was: Started)

Comment 10 by sheriffbot on Wed, Mar 4, 2020, 2:03 PM EST Project Member

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

Comment 11 by sheriffbot on Thu, Mar 5, 2020, 2:25 PM EST Project Member

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

Requesting merge to stable M80 because latest trunk commit (746613) appears to be after stable branch point (722274).

Requesting merge to beta M81 because latest trunk commit (746613) appears to be after beta branch point (737173).

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

Comment 12 by sheriffbot on Thu, Mar 5, 2020, 2:27 PM EST Project Member

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

This bug requires manual review: We are only 11 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
- 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 13 by hongchan@chromium.org on Thu, Mar 5, 2020, 2:48 PM EST Project Member

1. Yes. This is a security issue with an extra small fix.
2. https://chromium-review.googlesource.com/c/chromium/src/+/2082897
3. I might wait until tomorrow.
4. This is UaP P1 issue.
5. No.
6. N/A

If approved, I'll try M80 merge first tomorrow, and M81 merge next Wednesday.

Comment 14 by pbommana@google.com on Thu, Mar 5, 2020, 6:28 PM EST Project Member

Cc: adetaylor@chromium.org

+adetylor@(Security TPM)

Comment 15 by gov...@chromium.org on Thu, Mar 5, 2020, 6:37 PM EST Project Member

Labels: -Merge-Request-80 Merge-Rejected-80

We're not planning any further M80 releases, so rejecting merge to M80.

adetaylor@, please let me know if there is any concern here. Thank you.

Comment 16 by adetaylor@chromium.org on Thu, Mar 5, 2020, 6:41 PM EST Project Member

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

Agreed, this is something for M81. Approving merge to M81 branch 4044 as it's a simple fix. Please check there are no unexpected Canary crashes first.

Comment 17 by bugdroid on Fri, Mar 6, 2020, 3:12 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/+/eb377bd168cec1383d72c1ed2453d82bfbd67863

commit eb377bd168cec1383d72c1ed2453d82bfbd67863
Author: Hongchan Choi <hongchan@chromium.org>
Date: Fri Mar 06 20:10:36 2020

Use SupportsWeakPtr for messaging from rendering thread to main thread

In cross-thread messaging, the associated execution context can be
already gone 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.

(cherry picked from commit 913247c378d54e0378ffd09524e0aa7503035fc4)

Test: Locally confirmed that the repro does not crash.
~~Bug: 1057627~~
Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#746613}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2091596
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Cr-Commit-Position: refs/branch-heads/4044@{#692}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/eb377bd168cec1383d72c1ed2453d82bfbd67863/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/eb377bd168cec1383d72c1ed2453d82bfbd67863/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 18 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT Project Member

Labels: Release-0-M81

Comment 19 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:30 PM EDT Project Member

Labels: CVE-2020-6429 CVE_description-missing

Comment 20 by bugdroid on Sun, Mar 15, 2020, 9:39 PM EDT Project Member

Labels: merge-merged-3987 merge-merged-80

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/86ea13aba036daff052ed7b8351d181d10bbd4a2

commit 86ea13aba036daff052ed7b8351d181d10bbd4a2
Author: Hongchan Choi <hongchan@chromium.org>
Date: Mon Mar 16 01:38:40 2020

Use SupportsWeakPtr for messaging from rendering thread to main thread

In cross-thread messaging, the associated execution context can be
already gone 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.

Test: Locally confirmed that the repro does not crash.
~~Bug: 1057627~~
Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/heads/master@{#746613}
(cherry picked from commit 913247c378d54e0378ffd09524e0aa7503035fc4)

TBR=hongchan@chromium.org

Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104455
Commit-Queue: Krishna Govind <govind@chromium.org>
Reviewed-by: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1001}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/86ea13aba036daff052ed7b8351d181d10bbd4a2/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/86ea13aba036daff052ed7b8351d181d10bbd4a2/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 21 by bugdroid on Sun, Mar 15, 2020, 9:41 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/0919f62fc927aa5bdca6ff6df287d867137b794e

commit 0919f62fc927aa5bdca6ff6df287d867137b794e
Author: Krishna Govind <govind@chromium.org>
Date: Mon Mar 16 01:40:19 2020

Revert "Use SupportsWeakPtr for messaging from rendering thread to main thread"

This reverts commit 86ea13aba036daff052ed7b8351d181d10bbd4a2.

Reason for revert: Reverting by mistake skipped CQ

Original change's description:
> Use SupportsWeakPtr for messaging from rendering thread to main thread
>
> In cross-thread messaging, the associated execution context can be
> already gone 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.
>
> Test: Locally confirmed that the repro does not crash.
> ~~Bug: 1057627~~
> Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
> Commit-Queue: Hongchan Choi <hongchan@chromium.org>
> Reviewed-by: Raymond Toy <rtoy@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#746613}
> (cherry picked from commit 913247c378d54e0378ffd09524e0aa7503035fc4)
>
> TBR=hongchan@chromium.org
>
> Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104455
> Commit-Queue: Krishna Govind <govind@chromium.org>
> Reviewed-by: Krishna Govind <govind@chromium.org>
> Cr-Commit-Position: refs/branch-heads/3987@{#1001}
> Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

TBR=hongchan@chromium.org,govind@chromium.org

Change-Id: I7fa3714077e005f0e646a787bdf9fd79689c518c
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
~~Bug: 1057627~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104456
Reviewed-by: Krishna Govind <govind@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1002}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/0919f62fc927aa5bdca6ff6df287d867137b794e/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/0919f62fc927aa5bdca6ff6df287d867137b794e/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 22 by bugdroid on Mon, Mar 16, 2020, 1:53 AM EDT Project Member

Labels: merge-merged-3987_137

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/e650582b6e257aa4225c7b3136e38f7aa5ba1cde

commit e650582b6e257aa4225c7b3136e38f7aa5ba1cde
Author: Hongchan Choi <hongchan@chromium.org>
Date: Mon Mar 16 05:52:36 2020

Use SupportsWeakPtr for messaging from rendering thread to main thread

In cross-thread messaging, the associated execution context can be
already gone 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.

(cherry picked from commit 913247c378d54e0378ffd09524e0aa7503035fc4)

Test: Locally confirmed that the repro does not crash.
~~Bug: 1057627~~

Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#746613}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104662
Reviewed-by: Krishna Govind <govind@chromium.org>
Reviewed-by: Prudhvi Kumar Bommana <pbommana@google.com>
Cr-Commit-Position: refs/branch-heads/3987_137@{#5}
Cr-Branched-From: 55c16ce255e7a7feca588abeb4f082026b35e1ef-refs/branch-heads/3987@{#989}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/e650582b6e257aa4225c7b3136e38f7aa5ba1cde/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/e650582b6e257aa4225c7b3136e38f7aa5ba1cde/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 23 by 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 24 by bugdroid on Mon, Mar 16, 2020, 10:23 PM EDT Project Member

Labels: -merge-approved-80

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/958e0ed302abd12c797783950e3b14fab9c91d36

commit 958e0ed302abd12c797783950e3b14fab9c91d36
Author: Hongchan Choi <hongchan@chromium.org>
Date: Tue Mar 17 02:20:52 2020

Reland "Use SupportsWeakPtr for messaging from rendering thread to main thread"

This is a reland of 86ea13aba036daff052ed7b8351d181d10bbd4a2

Original change's description:
> Use SupportsWeakPtr for messaging from rendering thread to main thread
>
> In cross-thread messaging, the associated execution context can be
> already gone 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.
>
> Test: Locally confirmed that the repro does not crash.
> ~~Bug: 1057627~~
> Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2082897
> Commit-Queue: Hongchan Choi <hongchan@chromium.org>
> Reviewed-by: Raymond Toy <rtoy@chromium.org>
> Cr-Commit-Position: refs/heads/master@{#746613}
> (cherry picked from commit 913247c378d54e0378ffd09524e0aa7503035fc4)
>
> TBR=hongchan@chromium.org
>
> Change-Id: I51737594c918f6a4924c9a7ffe30db3e8de9a683
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104455
> Commit-Queue: Krishna Govind <govind@chromium.org>
> Reviewed-by: Krishna Govind <govind@chromium.org>
> Cr-Commit-Position: refs/branch-heads/3987@{#1001}
> Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

~~Bug: 1057627~~
Change-Id: I9c20dfc10160683b85dd2bba3e63aa9fd7e1c6c1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2106956
Reviewed-by: Krishna Govind <govind@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1013}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/958e0ed302abd12c797783950e3b14fab9c91d36/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.cc
[modify] https://crrev.com/958e0ed302abd12c797783950e3b14fab9c91d36/third_party/blink/renderer/modules/webaudio/audio_scheduled_source_node.h

Comment 25 by adetaylor@google.com on Tue, Mar 17, 2020, 11:17 AM EDT Project Member

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

Comment 26 by gov...@chromium.org on Tue, Mar 17, 2020, 4:33 PM EDT Project Member

Cc: prashanthpola@chromium.org

Comment 27 by adetaylor@chromium.org on Thu, Mar 19, 2020, 6:30 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 28 by adetaylor@google.com on Wed, Mar 25, 2020, 3:31 PM EDT Project Member

Cc: achuith@chromium.org

Comment 29 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