☆ Starred by 5 users

Owner:	hongchan@chromium.org **OOO (12.15-1.8)**
CC:	adetaylor@chromium.org carlosil@chromium.org rtoy@chromium.org pbomm...@chromium.org hongchan@chromium.org
Status:	Verified *(Closed)*
Components:	Blink>WebAudio
Modified:	Sep 22, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-Medium
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
merge-merged-4240
M-91
LTR-Merged-86
LTS-Security-86
Target-91
external_security_report
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
Release-0-M91
CVE-2021-30530

Issue 1201033: Security: Out-of-bounds access in WebAudio

Reported by kkwon...@gmail.com on Tue, Apr 20, 2021, 10:36 PM EDT

Code

VULNERABILITY DETAILS
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc;drc=7f5a8953f42e12194870ec6f0bf6d41c66663a36;l=173

```
bool AudioWorkletProcessor::PortTopologyMatches(
    v8::Isolate* isolate,
    v8::Local<v8::Context> context,
    const Vector<scoped_refptr<AudioBus>>& audio_port_1,
    const TraceWrapperV8Reference<v8::Array>& audio_port_2) {
  TRACE_EVENT0(TRACE_DISABLED_BY_DEFAULT("audio-worklet"),
               "AudioWorkletProcessor::Process (compare topology)");
  if (audio_port_2.IsEmpty())
    return false;

  // Two AudioPorts are supposed to have the same length because the number of
  // inputs and outputs of AudioNode cannot change after construction.
  v8::Local<v8::Array> port_2_local = audio_port_2.NewLocal(isolate);
  DCHECK(port_2_local->IsArray());
  DCHECK_EQ(audio_port_1.size(), port_2_local->Length());

  v8::TryCatch try_catch(isolate);

  v8::Local<v8::Value> value;
  uint32_t bus_index_counter = 0;
  for (const auto& audio_bus_1 : audio_port_1) {
    if (!port_2_local->Get(context, bus_index_counter).ToLocal(&value) ||       // *** 1 ***
        !value->IsArray())
      return false;

    // Compare the length of AudioBus1[i] from AudioPort1 and AudioBus2[i] from
    // AudioPort2.
    unsigned number_of_channels =
        audio_bus_1 ? audio_bus_1->NumberOfChannels() : 0;
    v8::Local<v8::Array> audio_bus_2 = value.As<v8::Array>();
    if (number_of_channels != audio_bus_2->Length())                             // *** 2 ***
      return false;

    // If the channel count of AudioBus1[i] and AudioBus2[i] matches, then
    // iterate all the channels in AudioBus1[i] and see if any AudioChannel
    // is detached. (i.e. transferred to a different thread)
    for (uint32_t channel_index = 0; channel_index < audio_bus_2->Length();
         ++channel_index) {
      if (!audio_bus_2->Get(context, channel_index).ToLocal(&value) ||
          !value->IsFloat32Array())                                              // *** 3 ***
        return false;
      v8::Local<v8::Float32Array> float32_array = value.As<v8::Float32Array>();

      // If any array is transferred, we need to rebuild them.
      if (float32_array->ByteLength() == 0)                                    // *** 4 ***
        return false;
    }

    bus_index_counter++;
  }

  return true;
}
```
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc;l=61;drc=cb83c85e1025099b2888bc29e24dac4ab49b02c7

```
bool AudioWorkletProcessor::Process(
    const Vector<scoped_refptr<AudioBus>>& inputs,
    Vector<scoped_refptr<AudioBus>>& outputs,
    const HashMap<String, std::unique_ptr<AudioFloatArray>>& param_value_map) {
  TRACE_EVENT0(TRACE_DISABLED_BY_DEFAULT("audio-worklet"),
               "AudioWorkletProcessor::Process");

  DCHECK(global_scope_->IsContextThread());
  DCHECK(!hasErrorOccurred());

  ScriptState* script_state =
      global_scope_->ScriptController()->GetScriptState();
  ScriptState::Scope scope(script_state);
  v8::Isolate* isolate = script_state->GetIsolate();
  v8::Local<v8::Context> context = script_state->GetContext();
  AudioWorkletProcessorDefinition* definition =
      global_scope_->FindDefinition(Name());

  // 1st JS arg |inputs_|. Compare |inputs| and |inputs_|. Then allocates the
  // data container if necessary.
  if (!PortTopologyMatches(isolate, context, inputs, inputs_)) {                  // *** 5 ***
```

https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc;drc=7f5a8953f42e12194870ec6f0bf6d41c66663a36;l=314

```
void AudioWorkletProcessor::CopyPortToArrayBuffers(
      v8::Isolate* isolate,
      const Vector<scoped_refptr<AudioBus>>& audio_port,
      BackingArrayBuffers& array_buffers) {
  DCHECK_EQ(audio_port.size(), array_buffers.size());

  for (uint32_t bus_index = 0; bus_index < audio_port.size(); ++bus_index) {
    const scoped_refptr<AudioBus>& audio_bus = audio_port[bus_index];
    size_t bus_length = audio_bus ? audio_bus->length() : 0;
    unsigned number_of_channels = audio_bus ? audio_bus->NumberOfChannels() : 0;
    for (uint32_t channel_index = 0; channel_index < number_of_channels;
         ++channel_index) {
      auto backing_store = array_buffers[bus_index][channel_index]               // *** 6 ***
                               .NewLocal(isolate)
                               ->GetBackingStore();
      memcpy(backing_store->Data(), audio_bus->Channel(channel_index)->Data(),  // *** 7 ***
             bus_length * sizeof(float));
    }
  }
}
```

The root cause of this vulnerability is JavaScript callback from [1].

In `AudioWorkletProcessor::PortTopologyMatches`, `audio_port_1` is the parameter variable `inputs` in `AudioWorkletProcessor::Process` [5].
The size of `audio_port_1` is the same as the length of `audio_bus_2` in most cases.
The variable `audio_bus_2` is determined by `audio_port_1` in `AudioWorkletProcessor::ClonePortTopology` function.
After `audio_bus_2` is set, `audio_bus_2` is not changed before `AudioWorkletProcessor::PortTopologyMatches` returns `false`.

When the user makes two `AudioWorkletNode`s using singleton pattern, `AudioWorkletNode`s have the same `AudioWorkletProcessor`.
Then, `AudioWorkletProcessor::PortTopologyMatches` can have different sizes of `audio_port_1`.
Because we can pass the different sizes of `inputs` using different `AudioWorkletNode`s.
It means that the length of `port_2_local` less than `bus_index_counter` which is an index of `audio_port_1`'s size.
In this case, we can make a JavaScript callback using `__defineGetter__`, and it will be called in [1].

Using the JavaScript callback, we can control the variable `value` which is the return value of the callback.
Then, we can bypass the check routine [2] because we can control the size of the array using the callback.
Also, we can bypass the check routines [3], and [4] in the same manner.
Bypassing the check routines, `AudioWorkletProcessor::PortTopologyMatches` always returns `true`.
It means the variable `audio_bus_2` is never changed, and also the variable `array_buffers`, which is explained as follows, is not changed too.

In `AudioWorkletProcessor::CopyPortToArrayBuffers`, `audio_port` is the same variable above `audio_port_1`.
The variable `array_buffers` is `Vector` type, and the size of `array_buffers` is also determined by `audio_port_1` from `AudioWorkletProcessor::ClonePortTopology`.
It means that the size of `audio_port_1` can be bigger than the size of `array_buffers` (using singleton pattern and bypassing check routines).
So we can access `array_buffers` out of bounds in [6].
Also, if we detach one of `ArrayBuffer` in `array_buffers` from `AudioWorkletProcessor::PortTopologyMatches` after bypassing check routines (TOCTOU),
We can access the detached backing store of `ArrayBuffer` in [7].

VERSION

Chrome Version: 90.0.4430.72 (latest stable version)
Operating System: Windows, Linux, MacOS, Android

REPRODUCTION CASE

I attached two JavaScript codes. One is Out-of-Bounds `Vector` access. The other is accessing the detached `ArrayBuffer`'s backing store.
Please see the attachments.

arraybuffer.html
1.4 KB View Download

oob.html
1.3 KB View Download

Comment 1 by sheriffbot on Tue, Apr 20, 2021, 10:37 PM EDT Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Thu, Apr 22, 2021, 10:05 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5667300636950528.

Comment 3 by ClusterFuzz on Thu, Apr 22, 2021, 10:06 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5079857089019904.

Comment 4 by carlosil@chromium.org on Fri, Apr 23, 2021, 7:53 PM EDT Project Member

Cc: carlosil@chromium.org
Labels: Needs-Feedback

It looks like CF was not able to reproduce this with either poc, and I was also not able to reproduce by hand. Could you attach the crash log you get? Thanks

Comment 5 by kkwon...@gmail.com on Sun, Apr 25, 2021, 9:56 PM EDT

I attach the crash logs. And, you have to run the PoCs with web server for reproducing it.

oob.log
10.9 KB View Download

arraybuffer.log
5.9 KB View Download

Comment 6 by sheriffbot on Sun, Apr 25, 2021, 9:58 PM EDT Project Member

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 7 by carlosil@chromium.org on Mon, Apr 26, 2021, 8:06 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: rtoy@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium
Components: Blink>WebAudio

rtoy: Can you please help triage this one too? Thanks

Comment 8 by rtoy@chromium.org on Tue, Apr 27, 2021, 12:55 PM EDT Project Member

Owner: hongchan@chromium.org
Cc: rtoy@chromium.org
Labels: OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2

See also ~~issue 1202060~~, which is probably a duplicate where DCHECK is enabled to catch the unexpected state which looks as if it can actually happen.

This probably happens for all OSes.

Comment 9 by sheriffbot on Tue, Apr 27, 2021, 1:03 PM EDT Project Member

Labels: M-91 Target-91

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

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

Comment 10 by sheriffbot on Tue, Apr 27, 2021, 1:39 PM EDT Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 sheriffbot on Wed, May 5, 2021, 12:21 PM EDT Project Member

hongchan: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 12 by hongchan@chromium.org on Wed, May 5, 2021, 6:29 PM EDT Project Member

Status: Started (was: Assigned)

Comment 13 by Git Watcher on Wed, May 5, 2021, 8:21 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49

commit f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49
Author: Hongchan Choi <hongchan@chromium.org>
Date: Thu May 06 00:20:54 2021

Return false when the size of audio_port_1 and audio_port_2 is different

The current code assumes the size of audio ports is identical because the number of inputs and outputs cannot change after construction. This assumption is broken when multiple AudioWorkletNodes share a singleton AudioWorkletProcessor instance.

This patch removes the assumption and explicitly returns false when the number of inputs and outputs does not match.

~~Bug: 1201033~~, ~~120260~~
Test: 3 repro cases submitted do not crash on ASAN.
Change-Id: I4065e7970b9b7b54468fc82558509a3238ff28e4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2875846
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/heads/master@{#879631}

[modify] https://crrev.com/f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49/third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc

Comment 14 by hongchan@chromium.org on Fri, May 7, 2021, 2:43 PM EDT Project Member
Status: Fixed (was: Started)

kkwondotnet@

Could you check with 92.0.4500.0?

Comment 15 by sheriffbot on Sat, May 8, 2021, 12:41 PM EDT Project Member
Labels: reward-topanel

Comment 16 by sheriffbot on Sat, May 8, 2021, 2:00 PM EDT Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 17 by sheriffbot on Sat, May 8, 2021, 2:25 PM EDT Project Member
Labels: Merge-Request-91

Requesting merge to beta M91 because latest trunk commit (879631) appears to be after beta branch point (738).

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

Comment 18 by sheriffbot on Sat, May 8, 2021, 2:27 PM EDT Project Member
Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 19 by kkwon...@gmail.com on Sun, May 9, 2021, 9:02 AM EDT

hongchan@

I checked it, and it seems to be fixed very well.

Comment 20 by hongchan@chromium.org on Mon, May 10, 2021, 11:30 AM EDT Project Member
Status: Verified (was: Fixed)

1. Yes.
2. https://crrev.com/c/2875846
3. Yes.
4. Yes.
5. This is a security issue.
6. No.
7. No.

Comment 21 by adetaylor@google.com on Mon, May 10, 2021, 3:17 PM EDT Project Member
Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91, branch 4472.

Comment 22 by adetaylor@chromium.org on Mon, May 10, 2021, 5:49 PM EDT Project Member
Cc: hongchan@chromium.org adetaylor@chromium.org pbomm...@chromium.org

~~Issue 1202060~~ has been merged into this issue.

Comment 23 by Git Watcher on Tue, May 11, 2021, 12:51 PM EDT Project Member
Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bce03b43e222a2e659809ae909674a242bdccdde

commit bce03b43e222a2e659809ae909674a242bdccdde
Author: Hongchan Choi <hongchan@chromium.org>
Date: Tue May 11 16:50:26 2021

Return false when the size of audio_port_1 and audio_port_2 is different

The current code assumes the size of audio ports is identical because
the number of inputs and outputs cannot change after construction. This
assumption is broken when multiple AudioWorkletNodes share a singleton
AudioWorkletProcessor instance.

This patch removes the assumption and explicitly returns false when the
number of inputs and outputs does not match.

(cherry picked from commit f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49)

~~Bug: 1201033~~, ~~120260~~
Test: 3 repro cases submitted do not crash on ASAN.
Change-Id: I4065e7970b9b7b54468fc82558509a3238ff28e4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2875846
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#879631}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885639
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4472@{#935}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/bce03b43e222a2e659809ae909674a242bdccdde/third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc

Comment 24 by amyressler@google.com on Thu, May 20, 2021, 1:08 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-7500

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 25 by amyressler@chromium.org on Thu, May 20, 2021, 5:34 PM EDT Project Member

Congratulations, the VRP Panel has decided to award you $7500 for this report! Nice work!

Comment 26 by amyressler@google.com on Fri, May 21, 2021, 5:32 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 27 by amyressler@chromium.org on Mon, May 24, 2021, 11:05 AM EDT Project Member

Labels: Release-0-M91

Comment 28 by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT Project Member

Labels: CVE-2021-30530 CVE_description-missing

Comment 29 by achuith@chromium.org on Thu, May 27, 2021, 3:24 PM EDT Project Member

Labels: LTS-Merge-Request-86 LTS-Security-86

Comment 30 by surabhigrover@chromium.org on Tue, Jun 1, 2021, 3:53 PM EDT Project Member

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 31 by Git Watcher on Wed, Jun 2, 2021, 2:35 PM EDT Project Member

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e80c2769e463f2795afa72fe36a66c02ba1f2a14

commit e80c2769e463f2795afa72fe36a66c02ba1f2a14
Author: Hongchan Choi <hongchan@chromium.org>
Date: Wed Jun 02 18:34:26 2021

Return false when the size of audio_port_1 and audio_port_2 is different

The current code assumes the size of audio ports is identical because
the number of inputs and outputs cannot change after construction. This
assumption is broken when multiple AudioWorkletNodes share a singleton
AudioWorkletProcessor instance.

This patch removes the assumption and explicitly returns false when the
number of inputs and outputs does not match.

(cherry picked from commit f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49)

~~Bug: 1201033~~, ~~120260~~
Test: 3 repro cases submitted do not crash on ASAN.
Change-Id: I4065e7970b9b7b54468fc82558509a3238ff28e4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2875846
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#879631}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2922863
Reviewed-by: Jana Grill <janagrill@google.com>
Commit-Queue: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1659}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/e80c2769e463f2795afa72fe36a66c02ba1f2a14/third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc

Comment 32 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 33 by vsavu@google.com on Mon, Jun 14, 2021, 12:27 PM EDT Project Member

Labels: -LTS-Merge-Approved-86 LTS-Merged-90 LTS-Merge-Request-90 LTS-Security-90

Comment 34 by gianluca@google.com on Tue, Jun 15, 2021, 6:28 AM EDT Project Member

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

Comment 35 by vsavu@google.com on Tue, Jun 15, 2021, 6:28 AM EDT Project Member

Labels: -LTS-Merged-90 LTR-Merged-86

Comment 36 by Git Watcher on Wed, Jun 16, 2021, 8:58 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/32bfec158a82ae94fb62efdd5dc2cd616f7c0891

commit 32bfec158a82ae94fb62efdd5dc2cd616f7c0891
Author: Hongchan Choi <hongchan@chromium.org>
Date: Wed Jun 16 12:57:57 2021

[M90-LTS] Return false when the size of audio_port_1 and audio_port_2 is different

The current code assumes the size of audio ports is identical because
the number of inputs and outputs cannot change after construction. This
assumption is broken when multiple AudioWorkletNodes share a singleton
AudioWorkletProcessor instance.

This patch removes the assumption and explicitly returns false when the
number of inputs and outputs does not match.

(cherry picked from commit f1e277f1b586e0be0cc7f3b4f6462fa4982b7b49)

(cherry picked from commit bce03b43e222a2e659809ae909674a242bdccdde)

~~Bug: 1201033~~, ~~120260~~
Test: 3 repro cases submitted do not crash on ASAN.
Change-Id: I4065e7970b9b7b54468fc82558509a3238ff28e4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2875846
Commit-Queue: Hongchan Choi <hongchan@chromium.org>
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#879631}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885639
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Original-Commit-Position: refs/branch-heads/4472@{#935}
Cr-Original-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2961288
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1525}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/32bfec158a82ae94fb62efdd5dc2cd616f7c0891/third_party/blink/renderer/modules/webaudio/audio_worklet_processor.cc

Comment 37 by vsavu@google.com on Wed, Jun 16, 2021, 9:04 AM EDT Project Member

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

Comment 38 by sheriffbot on Wed, Sep 22, 2021, 1:34 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

Comment 39 by amyressler@chromium.org on Wed, Sep 22, 2021, 2:16 PM EDT Project Member

Hello- we consider attachments/pocs included with reports to be an integral part of the report, so I've un-deleted them. Thanks!