


☆ Starred by 2 users

Owner:

 hongchan@chromium.org
OOO (12.15-1.8)

CC:

pbomm...@chromium.org
adetaylor@google.com
srinivassista@google.com
achuith@chromium.org

Status:

Verified (Closed)

Components:

Blink>WebAudio

Modified:

May 15, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

Linux, Windows, Chrome, Mac

Pri:

1

Type:

Bug-Security

Security_Impact-Stable
M-80
Security_Severity-High
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
VulnerabilityAnalysis-Requested
VulnerabilityAnalysis-Submitted
merge-merged-3987
merge-merged-80
Release-2-M80
CVE-2020-6384

Issue 1048473: Use-after-destroy in WebAudio

Reported by da...@davidmanouchehri.com on Mon, Feb 3, 2020, 10:35 PM EST

🔗 Code

VULNERABILITY DETAILS

Inside OfflineAudioContext::resumeContext, we can end up in a state where an uninitialized handler is called.

We can trigger this edge case through the following steps:

1. Create an iframe and append it to our document to get a new ExecutionContext
2. Create a OfflineAudioContext within our new iframe's ExecutionContext
3. Set a JS suspend handler on our OfflineAudioContext
4. Begin rendering our OfflineAudioContext with the JS startRendering() function
5. Once we hit the callback of the JS suspend handler, remove the iframe's ExecutionContext
6. The removal of the ExecutionContext calls ContextLifecycleObserver::ContextDestroyed -> AudioContext::ContextDestroyed -> AudioContext::Uninitialize() -> BaseAudioContext::Uninitialize()

Inside of BaseAudioContext::Uninitialize(), we can see our handlers being destroyed.

```
void BaseAudioContext::Uninitialize() {  
  ...  
  // This stops the audio thread and all audio rendering.  
  if (destination_node_)  
    destination_node_>Handler().Uninitialize();  
  ...  
  Clear();  
  ...  
}  
  
void BaseAudioContext::Clear() {  
  destination_node_.Clear();  
  // The audio rendering thread is dead. Nobody will schedule AudioHandler  
  // deletion. Let's do it ourselves.  
  GetDeferredTaskHandler().ClearHandlersToBeDeleted();  
  is_cleared_ = true;  
}
```

7. Now that our handlers have all been deleted, we can resume rendering on our OfflineAudioContext.

```
ScriptPromise OfflineAudioContext::resumeContext(ScriptState* script_state) {  
  ...  
  // If the context is suspended, resume rendering by setting the state to  
  // "Running", and calling startRendering(). Note that resuming is possible  
  // only after the rendering started.  
  SetContextState(kRunning);  
}
```

```
DestinationHandler().StartRendering()); // <----- We call an uninitialized handler here
...
}
```

VERSION

Chrome Version: Tested on 79.0.3945.79 + stable and 81.0.4040.5 + dev
Operating System: Any

REPRODUCTION CASE

Open audio.html in Chrome.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: Tab/renderer
Crash State:
[0203/214143.316062:INFO:CONSOLE(16)] "Removing the reference...", source: file:///home/dave/0days/chrome/0009/audio.html (16)
Received signal 11 SEGV_MAPERR 000000000080
#0 0x7fac4b1a2dc9 base::debug::CollectStackTrace()
#1 0x7fac4b0dd653 base::debug::StackTrace::StackTrace()
#2 0x7fac4b1a2970 base::debug::(anonymous namespace)::StackDumpSignalHandler()
#3 0x7fac32f1890 (/lib/x86_64-linux-gnu/libpthread-2.27.so+0x1288f)
#4 0x7fac40671d34 blink::BackgroundFetchRegistration::downloadTotal()
#5 0x7fac40a03f0f [0203/214143.317622:INFO:CONSOLE(18)] "Triggering access on the freed handlers, we should crash now.", source: file:///home/dave/0days/chrome/0009/audio.html (18)
blink::OfflineAudioContext::resumeContext()
#6 0x7fac40c7cbd0 blink::V8OfflineAudioContext::ResumeMethodCallback()
#7 0x7fac4161e182 v8::internal::FunctionCallbackArguments::Call()
#8 0x7fac4161d5e6 v8::internal::(anonymous namespace)::HandleApiCallHelper<>()
#9 0x7fac4161cb5f v8::internal::Builtin_Impl_HandleApiCall()
#10 0x7fac414f81b8 Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit
r8: 0000000000000000 r9: 0000000000000010 r10: 00002414082853f1 r11: 00007fac40a03f10
r12: 000034121d5e7438 r13: 00007ffd95ab6670 r14: 00007ffd95ab64d0 r15: 000037e6c42dd090
di: 0000000000000000 si: 0000000000000000 bp: 00007ffd95ab6480 bx: 00002aff2bef3718
dx: 0000241400000000 ax: 0000000000000000 cx: ffffffff00 sp: 00007ffd95ab6480
ip: 00007fac40671d34 efi: 000000000010202 cgf: 002b000000000033 erf: 0000000000000004
trp: 000000000000000e msk: 0000000000000000 cr2: 0000000000000080
[end of stack trace]

CREDIT INFORMATION

Reporter credit: David Manouchehri

[Deleted] **audio.html**

[Comment 1](#) by [da...@davidmanouchehri.com](#) on Mon, Feb 3, 2020, 10:36 PM EST

I believe [@hongchan](#) would be the correct person to assign the ticket to.

[Comment 2](#) by [da...@davidmanouchehri.com](#) on Mon, Feb 3, 2020, 10:40 PM EST

My suggested patch would be to set AudioContextState::kClosed in BaseAudioContext::Uninitialize.

[Comment 3](#) by [da...@davidmanouchehri.com](#) on Tue, Feb 4, 2020, 1:17 AM EST

This looks quite similar to these previous tickets, which were both rated at Security_Severity-High.

<https://bugs.chromium.org/p/chromium/issues/detail?id=977107>

<https://bugs.chromium.org/p/chromium/issues/detail?id=959700>

[Comment 4](#) by [ellyj...@chromium.org](#) on Tue, Feb 4, 2020, 9:31 AM EST

Status: Untriaged (was: Unconfirmed)

Cc: hongchan@chromium.org

Labels: OS-Chrome OS-Linux OS-Mac OS-Windows

Components: Blink>WebAudio

Mac triage: Marking for WebAudio triage, setting OS tags per original report. I can't evaluate SecSeverity or SecImpact.

[Comment 5](#) by [ClusterFuzz](#) on Tue, Feb 4, 2020, 5:01 PM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5740068334534656>.

[Comment 6](#) by [ClusterFuzz](#) on Tue, Feb 4, 2020, 7:20 PM EST

Labels: Security_Impact-Stable

Detailed Report: <https://clusterfuzz.com/testcase?key=5740068334534656>

Fuzzer:

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Null-dereference READ

Crash Address: 0x000000000060

Crash State:

blink::AudioNode::Handler

blink::OfflineAudioContext::resumeContext

blink::V8OfflineAudioContext::ResumeMethodCallback

Sanitizer: address (ASAN)

Crash Revision: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&revision=738333

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5740068334534656

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/5740068334534656> -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/Yh3qCYFvHj6E5jz5> so we can improve.

[Comment 7](#) Deleted

[Comment 8](#) by carlosil@chromium.org on Wed, Feb 5, 2020, 5:57 PM EST

Labels: Security_Severity-High

I still can't reproduce the use after destroy, only the null deref that Clusterfuzz triggers.

hongchan@: Could you take a look since this seems similar to crbug/977107? Thanks.

[Comment 9](#) by carlosil@chromium.org on Wed, Feb 5, 2020, 5:58 PM EST

Labels: M-80

[Comment 10](#) by carlosil@chromium.org on Wed, Feb 5, 2020, 6:07 PM EST

Status: Assigned (was: Untriaged)

[Comment 11](#) by carlosil@chromium.org on Wed, Feb 5, 2020, 6:07 PM EST

Owner: hongchan@chromium.org

Cc: -hongchan@chromium.org

[Comment 12](#) by sheriffbot@chromium.org on Thu, Feb 6, 2020, 11:47 AM EST

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 13](#) by hongchan@chromium.org on Thu, Feb 6, 2020, 12:52 PM EST

Status: Started (was: Assigned)

[Comment 14](#) by hongchan@chromium.org on Thu, Feb 6, 2020, 3:47 PM EST

Status: Fixed (was: Started)

I submitted a patch, but with a wrong issue:

<https://chromium-review.googlesource.com/c/chromium/src/+2042409>

[Comment 15](#) by hongchan@chromium.org on Thu, Feb 6, 2020, 3:47 PM EST

Do not resume OfflineAudioContext when it is cleared

Previously OfflineAudioContext::resumeContext() method did not check if the context is cleared by ExecutionContext::ContextDestroyed(). Such case is possible when the audio context is a part of a detached iframe.

This CL changes the check so we can verify if the context's resources is still available. Otherwise, we can reject the resume promise resolver.

Test: Locally confirmed ASAN does not crash with the repro case.

Bug: 1048373

Change-Id: I96a601dcf63963525d95cfc5089fd4a3b0176687

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2042409>

Commit-Queue: Hongchan Choi <hongchan@chromium.org>

Commit-Queue: Kentaro Hara <haraken@chromium.org>

Auto-Submit: Hongchan Choi <hongchan@chromium.org>

Reviewed-by: Kentaro Hara <haraken@chromium.org>

Cr-Commit-Position: refs/heads/master@{#739085}

[Comment 16](#) by hongchan@chromium.org on Fri, Feb 7, 2020, 11:24 AM EST

Status: Verified (was: Fixed)

The CF confirmed the case as fixed.

[Comment 17](#) by da...@davidmanouchehri.com on Fri, Feb 7, 2020, 11:36 AM EST

Nice! I can't reproduce the crash anymore either.

Is the patch straightforward enough to merge into M80? (Sorry for reporting right before the release.)

[Comment 18](#) by hongchan@chromium.org on Fri, Feb 7, 2020, 11:40 AM EST

Labels: Merge-Request-80

Yes. I'll try the request. Thanks for the report and confirmation, David!

[Comment 19](#) by ClusterFuzz on Fri, Feb 7, 2020, 12:22 PM EST

Detailed Report: <https://clusterfuzz.com/testcase?key=5740068334534656>

Fuzzer:

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Null-dereference READ

Crash Address: 0x000000000060

Crash State:

blink::AudioNode::Handler

blink::OfflineAudioContext::resumeContext

blink::V8OfflineAudioContext::ResumeMethodCallback

Sanitizer: address (ASAN)

Crash Revision: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&revision=738333

Fixed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=739084:739085

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5740068334534656

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/5740068334534656> -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 20 by srinivassista@google.com on Fri, Feb 7, 2020, 1:47 PM EST

Labels: Merge-Request-81

Adding merge-request-81 so this can be merged to M81 first and then based on coverage we can merge to M80

Comment 21 by hongchan@chromium.org on Fri, Feb 7, 2020, 1:48 PM EST

Is M81 4044?

Comment 22 by da...@davidmanouchehri.com on Fri, Feb 7, 2020, 2:35 PM EST

Should be, that's what OmahaProxy says.

Comment 23 by natashapabrai@google.com on Mon, Feb 10, 2020, 2:36 PM EST

Labels: reward-topanel

Comment 24 Deleted

Comment 25 by mmoroz@google.com on Tue, Feb 11, 2020, 11:51 AM EST

Labels: VulnerabilityAnalysis-Requested

hongchan@, 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 natashapabrai@google.com on Tue, Feb 11, 2020, 5:08 PM EST

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 27 by natashapabrai@google.com on Tue, Feb 11, 2020, 5:10 PM EST

Congrats! The Panel decided to award \$7,500 for this report!

Comment 28 by natashapabrai@google.com on Tue, Feb 11, 2020, 5:16 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 29 by da...@davidmanouchehri.com on Tue, Feb 11, 2020, 5:35 PM EST

Awesome! Do you have any feedback on how I could improve future reports?

Comment 30 by hongchan@chromium.org on Wed, Feb 12, 2020, 10:03 AM EST

Ping on the merge request 81.

Comment 31 by mmoroz@chromium.org on Thu, Feb 13, 2020, 12:06 PM EST

Labels: VulnerabilityAnalysis-Submitted

Comment 32 by adetaylor@google.com on Thu, Feb 13, 2020, 1:11 PM EST

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

Approved for M80 (branch:3987) and M81 (branch:4044), but please first check that everything looks good in Canary.

Apologies for not approving the merge earlier - we're undergoing a bit of a process change and this fell through a crack.

Comment 33 by hongchan@chromium.org on Thu, Feb 13, 2020, 1:15 PM EST

Oops. Sorry M81 is already done. I was asking for M80.

Also just confirmed that Canary looks fine when the stable (M80) crashed right away.

Comment 34 by bugdroid on Thu, Feb 13, 2020, 2:59 PM EST

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

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+c9eb9d07eda7bf3608167c63c4bf1a4e12176aef>

commit [c9eb9d07eda7bf3608167c63c4bf1a4e12176aef](https://chromium.googlesource.com/chromium/src.git/+c9eb9d07eda7bf3608167c63c4bf1a4e12176aef)

Author: Hongchan Choi <hongchan@chromium.org>

Date: Thu Feb 13 19:59:04 2020

Do not resume OfflineAudioContext when it is cleared

Previously OfflineAudioContext::resumeContext() method did not check if the context is cleared by ExecutionContext::ContextDestroyed().

Such case is possible when the audio context is a part of a detached iframe.

This CL changes the check so we can verify if the context's resources is still available. Otherwise, we can reject the resume promise resolver.

(cherry picked from commit [5d595814f7262727112fc068ad6d4bc9ec319df4](https://chromium.googlesource.com/chromium/src.git/+c9eb9d07eda7bf3608167c63c4bf1a4e12176aef))

Test: Locally confirmed ASAN does not crash with the repro case.

Bugs: [1048473](https://bugs.chromium.org/p/chromium/issues/detail?id=1048473)

Change-Id: [I96a601dcf63963525d95cfc5089fd4a3b0176687](https://chromium-review.googlesource.com/c/chromium/src/+2042409)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2042409>

Commit-Queue: Hongchan Choi <hongchan@chromium.org>

Commit-Queue: Kentaro Hara <haraken@chromium.org>

Auto-Submit: Hongchan Choi <hongchan@chromium.org>

Reviewed-by: Kentaro Hara <haraken@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#739085}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2055005>

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

Cr-Commit-Position: refs/branch-heads/3987@{#885}

Cr-Branch-From: [c4e8da9871cc266be74481e212f3a5252972509d](https://chromium-review.googlesource.com/c/chromium/src/+2055005)-refs/heads/master@{#72274}

[modify] https://crrev.com/c9eb9d07eda7bf3608167c63c4bf1a4e12176aef/third_party/blink/renderer/modules/webaudio/offline_audio_context.cc

[Comment 35](#) by da...@davidmanouchehri.com on Thu, Feb 13, 2020, 6:34 PM EST

This didn't make it into the 80.0.3987.106 release today, did it?

[Comment 36](#) by hongchan@chromium.org on Thu, Feb 13, 2020, 6:47 PM EST

I kinda doubt that given it is just landed few hours ago.

[Comment 37](#) by pbommana@google.com on Fri, Feb 14, 2020, 1:51 PM EST

[hongchan@](#) Please go ahead and merge the CL to branch 4044 (refs/branch-heads/4044) manually asap, so that this would be part of M81 Beta release next week.

[Comment 38](#) by hongchan@chromium.org on Fri, Feb 14, 2020, 1:57 PM EST

Sorry for the confusion, but it's already in 4044. The associated issue number was wrong, so it did not reflect here.

See: <https://chromium-review.googlesource.com/c/chromium/src/+2044479>

Do not resume OfflineAudioContext when it is cleared

Previously OfflineAudioContext::resumeContext() method did not check if the context is cleared by ExecutionContext::ContextDestroyed(). Such case is possible when the audio context is a part of a detached iframe.

This CL changes the check so we can verify if the context's resources is still available. Otherwise, we can reject the resume promise resolver.

(cherry picked from commit [5d595814f7262727112fc068ad6d4bc9ec319df4](#))

Test: Locally confirmed ASAN does not crash with the repro case.

Bug: 1048373

Change-Id: I96a601dcf63963525d95cfc5089fd4a3b0176687

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2042409>

Commit-Queue: Hongchan Choi <hongchan@chromium.org>

Commit-Queue: Kentaro Hara <haraken@chromium.org>

Auto-Submit: Hongchan Choi <hongchan@chromium.org>

Reviewed-by: Kentaro Hara <haraken@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#739085}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2044479>

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

Cr-Commit-Position: refs/branch-heads/4044@{#117}

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

[Comment 39](#) by [sheriffbot](#) on Fri, Feb 14, 2020, 7:50 PM EST

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

[Comment 40](#) by [sheriffbot](#) on Mon, Feb 17, 2020, 12:09 PM EST

Cc: srinivassista@google.com adetaylor@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 41](#) by hongchan@chromium.org on Tue, Feb 18, 2020, 11:20 AM EST

Once again, the fix is merged to both 4044 (M81) and 3987 (M80). See the [comment #38](#) and [#34](#) respectively.

[Comment 42](#) by [sheriffbot](#) on Tue, Feb 18, 2020, 12:08 PM EST

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 43](#) by pbommana@google.com on Tue, Feb 18, 2020, 12:23 PM EST

Cc: pbommana@google.com hongchan@chromium.org

Thank you so much [hongchan@](#), I think you mentioned the bug_id as 1048373 instead of 1048473, hence the sheriffbot thinks that the CL isn't merged.

Also as stated by sheriffbot can you please remove the merge-approved-81 label if all required merged have landed.

[Comment 44](#) by hongchan@chromium.org on Tue, Feb 18, 2020, 12:24 PM EST

Labels: -Merge-Approved-81

[Comment 45](#) Deleted

[Comment 46](#) by da...@davidmanouchehri.com on Tue, Feb 18, 2020, 2:42 PM EST

What's the CVE for this one? I don't see it mentioned in the release notes for 80.0.3987.116, but the bug is fixed now in stable.

https://chromereleases.googleblog.com/2020/02/stable-channel-update-for-desktop_18.html
<https://chromium.googlesource.com/chromium/src/+c9eb9d07eda7bf3608167c63c4bf14e12176aef>

[Comment 47](#) by adetaylor@google.com on Thu, Feb 20, 2020, 11:33 AM EST

Yes, apologies for a delay, I've been out of the office so the release notes will be a couple of days late.

[Comment 48](#) by da...@davidmanouchehri.com on Thu, Feb 20, 2020, 11:36 AM EST

No rush, just wanted to make sure it wasn't forgotten. 🙏

[Comment 49](#) by adetaylor@google.com on Thu, Feb 20, 2020, 12:50 PM EST

Labels: Release-2-M80

[Comment 50](#) by adetaylor@chromium.org on Thu, Feb 20, 2020, 1:22 PM EST

Labels: CVE-2020-6384 CVE_description-missing

[Comment 51](#) by adetaylor@chromium.org on Thu, Feb 27, 2020, 5:53 PM EST

Labels: -CVE_description-missing CVE_description-submitted

[Comment 52](#) by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST

Cc: achuith@chromium.org

[Comment 53](#) by [sheriffbot](#) on Fri, May 15, 2020, 2:56 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

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

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)