☆ Starred by 3 users

Owner:	rtoy@chromium.org **Email to this user bounced**
CC:	rtoy@chromium.org hongchan@chromium.org vulnd...@sourcefire.com
Status:	Fixed *(Closed)*
Components:	Blink>WebAudio
Modified:	May 19, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Needs-Feedback
Security_Impact-Stable
Security_Severity-High
reward-7500
allpublic
reward-inprocess
CVE_description-submitted
Target-88
M-88
Merge-Rejected-88
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
Release-0-M89
external_security_report
merge-merged-4389
merge-merged-89
CVE-2021-21160

Issue 1170531: Talos Security Advisory for Google Chrome browser (TALOS-2021-1235)

Reported by regiw...@sourcefire.com on Mon, Jan 25, 2021, 4:52 PM EST

Code

Google Chrome AudioDelayDSPKernel::ProcessKRate heap-based buffer overlow vulnerability

Summary

An exploitable heap-based buffer overflow vulnerability exists in Google Chromium browser at least in versions 89.0.4383.0 64-bit and 90.0.4390.0 64-bit. A specially crafted HTML web page can cause a heap-based Buffer Overflow condition, resulting in a remote code execution. The victim needs to visit malicious web site to trigger the vulnerability.

Tested Versions

Google Chrome ver 841401 (89.0.4383.0 64-bit)
Google Chrome ver 844161 (90.0.4390.0 64-bit)

Product URLs

https://www.google.com/chrome/

CVSSv3 Score

8.8 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE

CWE-122 - Heap-based Buffer Overflow

Details

Google Chrome is a cross-platform web browser, developed by Google.

To understand the vulnerability let us analyze some parts of the poc.html file and coresponding logged lines from the browser console:

```
 "Mutation nodes amount :  6"
 "[ 4:21:34 PM ] :: Connecting nodes"
 "[ 4:21:34 PM ] :: Nodes connected"
 "[ 4:21:34 PM ] :: MediaElementAudioSourceNode_handler"
 "[ 4:21:34 PM ] :: AudioContext_handler"
 "IIRFilterNode: state is bad, probably due to unstable filter."

 "[ 4:21:34 PM ] :: ScriptProcessorNode_oncomplete"
 "[ 4:21:34 PM ] :: Index : 1"
 "[ 4:21:34 PM ] :: Connect IIRFilterNode to DelayNode.delayTime"
```

As we can see, after an initialization phase of PoC setup, first events start to appear and being handle.
Crucial actions for our PoC take place inside the oncomplete event handler named ScriptProcessorNode_oncomplete of the ScriptProcessorNode node:

```
Line 42     var g_fuzzRandom_index = 0;
Line 43
Line 44     //events handlers
Line 45     function ScriptProcessorNode_oncomplete()
Line 46     {
Line 47         writeLog("ScriptProcessorNode_oncomplete");
Line 48
Line 49         g_fuzzRandom_index++;
Line 50         writeLog("Index : " + g_fuzzRandom_index);
Line 51
Line 52
Line 53         if(g_fuzzRandom_index == 1)
Line 54         {
Line 55             writeLog("Connect IIRFilterNode to DelayNode.delayTime");
Line 56             audioNodesObjects.mutation[4].obj.connect( audioNodesObjects.mutation[5].obj.delayTime );
Line 57             return;
Line 58         }
```

During the first execution of ScriptProcessorNode_oncomplete event handler IIRFilterNode node is being connected to an AudioParam object. In our case it is a delayTime field of DelayNode object line 56.
That connection is required to trigger the vulnerability but tests have shown that beside IIRFilterNode a different type of AudioNode can be also use to obtain the same result.

When the ScriptProcessorNode_oncomplete handler is executed for a second time, the following lines will appear inside the log file:

```
 "[ 4:21:35 PM ] :: ScriptProcessorNode_oncomplete"
 "[ 4:21:35 PM ] :: Index : 2"
 "[ 4:21:35 PM ] :: Switch delayTime of DelayNode to k-rate"
```

and the corresponding code is executed :

```
Line 59 if(g_fuzzRandom_index == 2)
Line 60 {
Line 61     //DelayNode
Line 62     writeLog("Switch delayTime of DelayNode to k-rate");
Line 63     audioNodesObjects.mutation[5].obj.delayTime.automationRate = "k-rate";
Line 64     return;
Line 65 }
```

The crucial code is executed in line 63 where value of automationRate field is changed to k-rate from a-rate.
More details about possible AutomationRate values are available here: https://www.w3.org/TR/webaudio/#dom-audioparam-automationrate
That switch during processing phase (we are inside oncomplete event handler) leads to the vulnerability inside blink::AudioDelayDSPKernel::ProcessKRate method located in file third_party\blink\renderer\platform\audio\audio_delay_dsp_kernel.cc.
As you might notice browsing code around blink::AudioDelayDSPKernel::ProcessKRate there is also method responsible of data procesing in case when automationRate field is set to a-rate and its called AudioDelayDSPKernel::ProcessARate.
As I mentioned before, it seems to runtime change from "a-rate" to "k-rate" during processing phase have lead to internal state confusion of the DelayNode object and finally to the vulnerability in :

audio_delay_dsp_kernel.cc

```
Line 276   // Now copy out the samples from the buffer, starting at the read pointer,
Line 277   // carefully handling wrapping of the read pointer.
Line 278   float* read_pointer = &buffer[read_index1];
Line 279
Line 280   int remainder = buffer_end - read_pointer;
Line 281   memcpy(sample1, read_pointer,
Line 282          sizeof(*sample1) *
Line 283              std::min(static_cast<int>(frames_to_process), remainder));
```

There is no check whether buffer_end is smaller than read_pointer which in our case happens. Further in line 281 as a size parameter for memcpy the smaller value of frames_to_process and reminder is selected.
Because both variables are treated as a signed integer our remainder ends up beeing selected because its value is < 0. At the end its casted to size_t (unsigned value) what finally cause an attempt to copy a huge amount of memory.

Proper heap grooming can give an attacker full control of this heap overflow vulnerability and as a result could allow it to be turned into a arbitrary code execution.

Crash Information

```
=================================================================
==1076==ERROR: AddressSanitizer: negative-size-param: (size=-8589824196)
    #0 0x7ff74867402f in __asan_memcpy C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_interceptors_memintrinsics.cpp:22
    #1 0x7ffaf2dc9ab1 in blink::AudioDelayDSPKernel::ProcessKRate(float const *, float *, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\audio\audio_delay_dsp_kernel.cc:281:3
    #2 0x7ffaf2dcf38c in blink::AudioDSPKernelProcessor::Process(class blink::AudioBus const *, class blink::AudioBus *, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\audio\audio_dsp_kernel_processor.cc:85:20
    #3 0x7ffaf23dfbac in blink::AudioBasicProcessorHandler::Process(unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\audio_basic_processor_handler.cc:85:18
    #4 0x7ffaf0be1e26 in blink::AudioHandler::ProcessIfNecessary(unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\audio_node.cc:368:7
    #5 0x7ffaf18a8f2c in blink::AudioNodeOutput::Pull(class blink::AudioBus *, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\audio_node_output.cc:137:13
    #6 0x7ffaf18abfe6 in blink::AudioNodeInput::SumAllConnections(class scoped_refptr<class blink::AudioBus>, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\audio_node_input.cc:128:40
    #7 0x7ffaf18ac278 in blink::AudioNodeInput::Pull(class blink::AudioBus *, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\audio_node_input.cc:158:3
    #8 0x7ffaf1953707 in blink::RealtimeAudioDestinationHandler::Render(class blink::AudioBus *, unsigned int, struct blink::AudioIOPosition const &, struct
blink::AudioCallbackMetric const &) C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\webaudio\realtime_audio_destination_node.cc:207:18
    #9 0x7ffaf23c15a7 in blink::AudioDestination::RequestRender(unsigned __int64, unsigned __int64, double, double, unsigned __int64)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\audio\audio_destination.cc:251:17
    #10 0x7ffaf23c03f4 in blink::AudioDestination::Render(class blink::WebVector<float *> const &, unsigned __int64, double, double, unsigned __int64)
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\audio\audio_destination.cc:194:5
    #11 0x7ffaedebee86 in content::RendererWebAudioDeviceImpl::Render(class base::TimeDelta, class base::TimeTicks, int, class media::AudioBus *)
C:\b\s\w\ir\cache\builder\src\content\renderer\media\renderer_webaudiodevice_impl.cc:253:21
    #12 0x7ffada23aef4 in media::SilentSinkSuspender::Render(class base::TimeDelta, class base::TimeTicks, int, class media::AudioBus *)
C:\b\s\w\ir\cache\builder\src\media\base\silent_sink_suspender.cc:84:14
    #13 0x7ffada171b16 in media::AudioOutputDeviceThreadCallback::Process(unsigned int)
C:\b\s\w\ir\cache\builder\src\media\audio\audio_output_device_thread_callback.cc:80:21
    #14 0x7ffada15810f in media::AudioDeviceThread::ThreadMain(void) C:\b\s\w\ir\cache\builder\src\media\audio\audio_device_thread.cc:95:18
    #15 0x7ffae1c7f18f in base::`anonymous namespace'::ThreadFunc C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:111:13
    #16 0x7ff74867e3a8 in __asan::AsanThread::ThreadStart(unsigned __int64, struct __sanitizer::atomic_uintptr_t *) C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:273
    #17 0x7ffba61a7c23  (C:\WINDOWS\System32\KERNEL32.DLL+0x180017c23)
    #18 0x7ffba7ced4d0  (C:\WINDOWS\SYSTEM32\ntdll.dll+0x18006d4d0)
```

Credit

Discovered by Marcin 'Icewall' Noga of Cisco Talos.

https://talosintelligence.com/vulnerability_reports/

Comment 1 Deleted

Comment 2 by regiw...@sourcefire.com on Mon, Jan 25, 2021, 4:59 PM EST

Please add access to vulndiscovery@sourcefire.com

Comment 3 by lgrey@chromium.org on Tue, Jan 26, 2021, 11:03 AM EST

Cc: rtoy@chromium.org
Labels: -OS-Mac OS-Windows Type-Bug-Security

[Mac triage] changing label to Windows based on stack trace in c#0

Comment 4 by sheriffbot on Tue, Jan 26, 2021, 11:07 AM EST

Labels: external_security_report

Comment 5 by rtoy@chromium.org on Tue, Jan 26, 2021, 12:41 PM EST

Cc: vulnd...@sourcefire.com
Labels: Needs-Feedback OS-Android OS-Chrome OS-Linux OS-Mac
Components: Blink>WebAudio

Where is the repro case? That would be very helpful.

This code is used on all platforms so likely also affects all platforms (except iOS of course).

Comment 6 by vulnd...@sourcefire.com on Tue, Jan 26, 2021, 1:01 PM EST

poc file added

poc.zip
27.0 KB Download

TALOS-2021-1235 - Google_Chrome_AudioDelayDSPKernel::ProcessKRate_heap-based_buffer_overlow_vulnerability.txt
9.2 KB View Download

Comment 7 by rtoy@chromium.org on Tue, Jan 26, 2021, 1:10 PM EST

Cc: hongchan@chromium.org

Comment 8 by rsleevi@chromium.org on Tue, Jan 26, 2021, 7:17 PM EST

Adding the contents of the zip file directly.

utilsAudio.js
1.5 KB View Download

README.md
332 bytes View Download

random.js
1.8 KB View Download

poc.html
6.0 KB View Download

nodesDefinitions.js
3.6 KB View Download

demicmAudioShort.mp3
22.4 KB Download

Comment 9 by ClusterFuzz on Tue, Jan 26, 2021, 7:17 PM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5669169327833088.

Comment 10 by rtoy@chromium.org on Thu, Jan 28, 2021, 2:33 PM EST

Thanks for the poc. I can reproduce this on my linux box. Not sure why clusterfuzz can't reproduce this.

Comment 11 by rtoy@chromium.org on Thu, Jan 28, 2021, 4:20 PM EST

Status: Started (was: Unconfirmed)
Owner: rtoy@chromium.org

Thanks for excellent analysis. The main thread changes the automation rate, but the audio thread could be in the middle of processing the AudioParam. These need to be coordinated better. I think the solution is that the main thread must wait until the audio thread is done processing before the rate is changed.

Implementing this now.

Comment 12 by rtoy@chromium.org on Thu, Jan 28, 2021, 7:01 PM EST

Adding a bunch of prints and stuff shows that the real problem is that the delay time AudioParam is NaN. Probably because the IIRFilter is possibly unstable.

I had a CL a while ago to make all AudioParams force NaN and infinity to the AudioParam.defaultValue. That was rejected. I'll have to try something else.

Comment 13 by rtoy@chromium.org on Fri, Jan 29, 2021, 12:38 PM EST

I also see that the random coefficients used for the IIRFilter can cause a DCHECK failure estimating the roots. I'll need to file a new issue on that.

Comment 14 by rtoy@chromium.org on Fri, Jan 29, 2021, 12:54 PM EST

Oops. I meant biquad not IIRFilter.

Comment 15 by rtoy@chromium.org on Fri, Jan 29, 2021, 1:49 PM EST

Converting the NaN values in an AudioParam to the default value (as specified in https://webaudio.github.io/web-audio-api/#computation-of-value) fixes this issue. I can't get a crash anymore.

I still think your analysis does point to a problem, but without a repro case, it's hard to say and even harder to verify that it's fixed.

Comment 16 by ClusterFuzz on Mon, Feb 1, 2021, 1:40 PM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6190435751231488.

Comment 17 by tsepez@chromium.org on Thu, Feb 4, 2021, 7:23 PM EST

Labels: Security_Impact-Stable Security_Severity-High Pri-1

Updating a couple of labels. Feel free to let me know if I've misjudged the situation. Thanks!

Comment 18 by sheriffbot on Fri, Feb 5, 2021, 12:48 PM EST

Labels: Target-88 M-88

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 19 by bugdroid on Mon, Feb 8, 2021, 12:13 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ab1862017b5717271a28376659944dddc602195c

commit ab1862017b5717271a28376659944dddc602195c
Author: Raymond Toy <rtoy@chromium.org>
Date: Mon Feb 08 17:13:08 2021

Convert AudioParam NaN values to the default value

If any output value of an AudioParam (including the intrinsic values
and any inputs to the AudioParam), should be NaN, replace the NaN
value with the associated defaultValue.

This causes some slowdowns so SIMD/NEON code was added to mitigate the
degradation. There is still some slowdown, but the worst case is now
about 7% slower on x86 and 10% on arm. Generally, the slowdown is less
than 2% and 5%, respectively. (Perversely, some results got faster,
and the differences are statistically significant.)

Full details can be found at
https://docs.google.com/spreadsheets/d/1EhbLHm-9cUoEO5aj1vYemVBLQ3Dh4dCJPPLTfZPrZt4/edit?usp=sharing

Manually tested the test case from the bug and the issue no longer
occurs.

~~Bug: 1170531~~
Change-Id: I00d902b40a9ef9da990c6d68b664b1dcfc31b091
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2658724
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Cr-Commit-Position: refs/heads/master@{#851733}

[modify] https://crrev.com/ab1862017b5717271a28376659944dddc602195c/third_party/blink/renderer/modules/webaudio/audio_param.cc
[add] https://crrev.com/ab1862017b5717271a28376659944dddc602195c/third_party/blink/web_tests/external/wpt/webaudio/the-audio-api/the-audioparam-interface/nan-param.html

Comment 20 by rtoy@chromium.org on Tue, Feb 9, 2021, 1:59 PM EST

Status: Fixed (was: Started)

Comment 21 by rtoy@chromium.org on Tue, Feb 9, 2021, 2:00 PM EST

Fix has baked for a day so I think it's good to go.

Comment 22 by sheriffbot on Tue, Feb 9, 2021, 2:18 PM EST

Labels: Merge-Request-89 Merge-Request-88

Requesting merge to stable M88 because latest trunk commit (851733) appears to be after stable branch point (827102).

Requesting merge to beta M89 because latest trunk commit (851733) appears to be after beta branch point (843830).

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

Comment 23 by sheriffbot on Tue, Feb 9, 2021, 2:19 PM EST

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89'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), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 24 by adetaylor@google.com on Tue, Feb 9, 2021, 4:41 PM EST

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389.

Comment 25 by rtoy@chromium.org on Tue, Feb 9, 2021, 5:25 PM EST

1. Does your merge fit within the Merge Decision Guidelines?
Yes.

2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2658724

3. Has the change landed and been verified on ToT?
Yes. Did a local build with ToT and retested. Repro case no longer does.

4. Does this change need to be merged into other active release branches (M-1, M+1)?
Should merge to 89, possibly 88 as well.

5. Why are these changes required in this milestone after branch?
Security issue due to writing past the bounds of an array. This is explained very well in c#0.

6. Is this a new feature?
No.

Comment 26 by bugdroid on Wed, Feb 10, 2021, 12:34 AM EST

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/eb0c0353bf245885797d8ce0d1b864d88a381fbb

commit eb0c0353bf245885797d8ce0d1b864d88a381fbb
Author: Raymond Toy <rtoy@chromium.org>
Date: Wed Feb 10 05:34:49 2021

Convert AudioParam NaN values to the default value

If any output value of an AudioParam (including the intrinsic values
and any inputs to the AudioParam), should be NaN, replace the NaN
value with the associated defaultValue.

This causes some slowdowns so SIMD/NEON code was added to mitigate the
degradation. There is still some slowdown, but the worst case is now
about 7% slower on x86 and 10% on arm. Generally, the slowdown is less
than 2% and 5%, respectively. (Perversely, some results got faster,
and the differences are statistically significant.)

Full details can be found at
https://docs.google.com/spreadsheets/d/1EhbLHm-9cUoEO5aj1vYemVBLQ3Dh4dCJPPLTfZPrZt4/edit?usp=sharing

Manually tested the test case from the bug and the issue no longer
occurs.

(cherry picked from commit ab1862017b5717271a28376659944dddc602195c)

~~Bug: 1170531~~
Change-Id: I00d902b40a9ef9da990c6d68b664b1dcfc31b091
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2658724
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#851733}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2686369
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#880}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/eb0c0353bf245885797d8ce0d1b864d88a381fbb/third_party/blink/renderer/modules/webaudio/audio_param.cc
[add] https://crrev.com/eb0c0353bf245885797d8ce0d1b864d88a381fbb/third_party/blink/web_tests/external/wpt/webaudio/the-audio-api/the-audioparam-interface/nan-param.html

Comment 27 by sheriffbot on Wed, Feb 10, 2021, 12:42 PM EST

Labels: reward-topanel

Comment 28 by sheriffbot on Wed, Feb 10, 2021, 1:57 PM EST

Labels: Restrict-View-SecurityNotify

Comment 29 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:27 PM EST

I'm not going to approve merge to M88 just yet; I think new and exciting SIMD code probably requires a few more days' bake time before rolling out to stable. That probably means this will actually ship in the initial M89 release but we'll see how things go.

Comment 30 by amyressler@google.com on Wed, Feb 17, 2021, 7:12 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 31 by amyressler@google.com on Wed, Feb 17, 2021, 7:21 PM EST

Congratulations, Cisco Talos team (especially Icewall)! The VRP Panel had decided to award y'all $7,500 for this report. Thanks for your submission and nice work!

Comment 32 by regiw...@sourcefire.com on Thu, Feb 18, 2021, 9:42 AM EST

Thank you for the update and reward. What is the timeline for disclosure release?

Comment 33 by amyressler@google.com on Thu, Feb 18, 2021, 9:57 AM EST

Hi, regiwils@ - in most cases (unless there is a notable exception) we make the reports public 14 weeks after report status is updated to Fixed.

Comment 34 by awhalley@google.com on Fri, Feb 19, 2021, 5:34 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 35 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST

Labels: Release-0-M89

Comment 36 by adetaylor@google.com on Fri, Feb 26, 2021, 4:44 PM EST

Labels: -Merge-Request-88 Merge-Rejected-88

Not merging to M88 - no further releases planned.

Comment 37 by asumaneev@google.com on Mon, Mar 1, 2021, 2:49 PM EST

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

Comment 38 by adetaylor@google.com on Mon, Mar 1, 2021, 7:26 PM EST

Labels: CVE-2021-21160 CVE_description-missing

Comment 39 by gianluca@google.com on Tue, Mar 2, 2021, 9:04 AM EST

Labels: LTS-Merge-Approved-86

Comment 40 by asumaneev@google.com on Tue, Mar 2, 2021, 9:07 AM EST

Labels: -LTS-Merge-Request-86

Comment 41 by bugdroid on Tue, Mar 2, 2021, 10:17 AM EST

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3910c9f5cde621b957349209a80cc524dea74b71

commit 3910c9f5cde621b957349209a80cc524dea74b71
Author: Raymond Toy <rtoy@chromium.org>
Date: Tue Mar 02 15:15:29 2021

Convert AudioParam NaN values to the default value

If any output value of an AudioParam (including the intrinsic values
and any inputs to the AudioParam), should be NaN, replace the NaN
value with the associated defaultValue.

This causes some slowdowns so SIMD/NEON code was added to mitigate the
degradation. There is still some slowdown, but the worst case is now
about 7% slower on x86 and 10% on arm. Generally, the slowdown is less
than 2% and 5%, respectively. (Perversely, some results got faster,
and the differences are statistically significant.)

Full details can be found at
https://docs.google.com/spreadsheets/d/1EhbLHm-9cUoEO5aj1vYemVBLQ3Dh4dCJPPLTfZPrZt4/edit?usp=sharing

Manually tested the test case from the bug and the issue no longer
occurs.

(cherry picked from commit ab1862017b5717271a28376659944dddc602195c)

(cherry picked from commit eb0c0353bf245885797d8ce0d1b864d88a381fbb)

~~Bug: 1170531~~
Change-Id: I00d902b40a9ef9da990c6d68b664b1dcfc31b091
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2658724
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#851733}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2686369
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4389@{#880}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2727697
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1551}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/3910c9f5cde621b957349209a80cc524dea74b71/third_party/blink/renderer/modules/webaudio/audio_param.cc
[add] https://crrev.com/3910c9f5cde621b957349209a80cc524dea74b71/third_party/blink/web_tests/external/wpt/webaudio/the-audio-api/the-audioparam-interface/nan-param.html

Comment 42 by asumaneev@google.com on Tue, Mar 2, 2021, 10:21 AM EST

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 43 by vulnd...@sourcefire.com on Wed, Mar 3, 2021, 9:49 AM EST

Please update the credits on https://chromereleases.googleblog.com/ for this bug to be "Marcin 'Icewall' Noga of Cisco Talos" rather than Aleksandar Nikolic

Comment 44 by amyressler@google.com on Wed, Mar 3, 2021, 10:55 AM EST

vulndiscovery@ - sure thing! Apologies we didn't catch that in our updates process. It will be updated on the release notes blog later today.

Comment 45 by vulnd...@sourcefire.com on Wed, Mar 3, 2021, 1:29 PM EST

Label: reward_to-manoga_at_cisco.com

Comment 46 by amyressler@google.com on Wed, Mar 3, 2021, 5:59 PM EST

Hello vulndiscovery@sourcefire folks, I see the reward-to label update from earlier today from y'all. Unfortunately, since the reward decision was made last week on this report, the payment process is already in progress and is associated with the regiwils@sourcefire account. Hopefully, there are no issues with transferring that reward internally on your side.
In the future, to ensure payment to an individual researcher on your team, it would be best to report that bug from an individual email address that is aligned to or can be tied to that researcher on your team through our payment process.
Please reach out with any questions or concerns.

Comment 47 by vulnd...@sourcefire.com on Wed, Mar 3, 2021, 8:05 PM EST

Sadly we can't facilitate any transfers, there are tax implications to this especially since Marcin is in another country. We can't submit from individual email addresses, that would make it impossible for us to track any of this. Please reassign the bounty.

Comment 48 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST

Labels: -CVE_description-missing CVE_description-submitted

Comment 49 by amyressler@google.com on Wed, Mar 10, 2021, 5:01 PM EST

vulndiscovery@ due to the details and complexities of the payment situation in our efforts to redirect the reward payment, I've sent a response off-bug via email.

Comment 50 by vulnd...@sourcefire.com on Fri, Apr 9, 2021, 9:59 AM EDT

What is the planned release date?

Comment 51 by amyressler@chromium.org on Fri, Apr 9, 2021, 10:59 AM EDT

The patch was part of the M89 milestone release and the bug will be made public 14 weeks after fix (which was as of 9 February), which is around 18 May, if my math is correct.

Comment 52 by sheriffbot on Wed, May 19, 2021, 1:50 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