




[chromium](#) ▾[New issue](#)[Open issues](#) ▾[Sign in](#)

★ Starred by 4 users

Owner:

 toprice@chromium.org
Deprecated. Using herre@google.com

CC:

 danakj@chromium.org
tommi@chromium.org
 toprice@chromium.org
adetaylor@chromium.org
hbos@chromium.org
wfh@chromium.org
herre@google.com
dcheng@chromium.org
eladalon@chromium.org

Status:Fixed (*Closed*)**Components:**[Blink>GetUserMedia](#)**Modified:**

Jul 29, 2022

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:[Linux](#), [Windows](#), [Chrome](#), [Mac](#)**Pri:**

1

Type:[Bug-Security](#)

[Hotlist-Merge-Review](#)
[reward-5000](#)
[Arch-x86_64](#)
[Deadline-Exceeded](#)
[Hotlist-Merge-Approved](#)
[Security_Severity-High](#)
[allpublic](#)
[reward-inprocess](#)
[Via-Wizard-Security](#)
[CVE_description-submitted](#)
[external_security_report](#)
[Target-94](#)
[Target-93](#)
[M-96](#)
[Target-96](#)
[FoundIn-92](#)
[FoundIn-93](#)

**Issue 1238209: container-overflow in blink::UserMediaProcessor::DetermineExistingAudioSessionId**Reported by emily...@gmail.com on Tue, Aug 10, 2021, 12:46 AM EDT[↪](#) Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Steps to reproduce the problem:

Chrome Version:

Chromium 93.0.4573.0

Google Chrome 94.0.4595.0 dev

1 ./chrome --user-data-dir=/tmp/xx --incognito --use-fake--for-media-stream --use-fake-device-for-media-stream --enable-experimental-web-platform-features <http://localhost:8000/main.html>

2 Click "allow use your microphone".

4 Click "allow use your camera".

5 Then the crash should happen immediately.

What is the expected behavior?

What went wrong?

=====

==1==ERROR: AddressSanitizer: container-overflow on address 0x7e88c0edc2e8 at pc 0x555b96708218 bp 0x7ffd1fcd9d90 sp 0x7ffd1fcd9d88

READ of size 8 at 0x7e88c0edc2e8 thread T0 (chrome)

==1==WARNING: invalid path to external symbolizer!

==1==WARNING: Failed to use and restart external symbolizer!

error: unknown argument '--demangle=True'

#0 0x555b96708217 in blink::UserMediaProcessor::DetermineExistingAudioSessionId()

./././third_party/blink/renderer/platform/heap/impl/member.h:257

#1 0x555b96708217 in operator blink::MediaStreamSource *

./././third_party/blink/renderer/platform/heap/impl/member.h:187

#2 0x555b96708217 in DetermineExistingAudioSessionId

./././third_party/blink/renderer/modules/mediastream/user_media_processor.cc:737

#3 0x555b96708217 in ?? ??:0

#4 0x555b96709afb in blink::UserMediaProcessor::SelectVideoDeviceSettings(blink::UserMediaRequest*, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>)

./././third_party/blink/renderer/modules/mediastream/user_media_processor.cc:874

#5 0x555b96709afb in ?? ??:0

#6 0x555b96729edf in void base::internal::InvokeHelper<true, void>::MakeItSo<void (blink::UserMediaProcessor::*)(blink::UserMediaRequest*, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>), blink::WeakPersistent<blink::UserMediaProcessor>, blink::Persistent<blink::UserMediaRequest>, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator> >(void

(blink::UserMediaProcessor::*&&)(blink::UserMediaRequest*, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>), blink::WeakPersistent<blink::UserMediaProcessor>&&, blink::Persistent<blink::UserMediaRequest>&&, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>&&)

(blink::UserMediaProcessor::*&&)(blink::UserMediaRequest*, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>), blink::WeakPersistent<blink::UserMediaProcessor>&&, blink::Persistent<blink::UserMediaRequest>&&, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0u, WTF::PartitionAllocator>&&)

./././base/bind_internal.h:509
#7 0x555b96729edf in MakeItSo<void (blink::UserMediaProcessor::*)(blink::UserMediaRequest *, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0, WTF::PartitionAllocator>), blink::WeakPersistent<blink::UserMediaProcessor>, blink::Persistent<blink::UserMediaRequest>, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0, WTF::PartitionAllocator>&&)

(blink::UserMediaProcessor::*&&)(blink::UserMediaRequest *, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0, WTF::PartitionAllocator>), blink::WeakPersistent<blink::UserMediaProcessor>, blink::Persistent<blink::UserMediaRequest>, WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0, WTF::PartitionAllocator>&&)

```

WTF::Vector<mojo::StructPtr<blink::mojom::blink::VideoInputDeviceCapabilities>, 0, WTF::PartitionAllocator> >
./././base/bind_internal.h:668
#8 0x555b96729edf in ?? ??:0
#9 0x555b825c6ed9 in
blink::mojom::blink::MediaDevicesDispatcherHost_GetVideoInputCapabilities_ForwardToCallback::Accept(mojo::Message*)
./././base/callback.h:98
#10 0x555b825c6ed9 in Accept ./gen/third_party/blink/public/mojom/mediastream/media_devices.mojom-blink.cc:928
#11 0x555b825c6ed9 in ?? ??:0
#12 0x555b860d7b55 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
./././mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:893
#13 0x555b860d7b55 in ?? ??:0
#14 0x555b860e9181 in mojo::MessageDispatcher::Accept(mojo::Message*)
./././mojo/public/cpp/bindings/lib/message_dispatcher.cc:43
#15 0x555b860e9181 in ?? ??:0
#16 0x555b860db657 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
./././mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:655
#17 0x555b860db657 in ?? ??:0
#18 0x555b860f4f23 in
mojo::internal::MultiplexRouter::ProcessIncomingMessage(mojo::internal::MultiplexRouter::MessageWrapper*,
mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*)
./././mojo/public/cpp/bindings/lib/multiplex_router.cc:1099
#19 0x555b860f4f23 in ?? ??:0
#20 0x555b860f3479 in mojo::internal::MultiplexRouter::Accept(mojo::Message*)
./././mojo/public/cpp/bindings/lib/multiplex_router.cc:719
#21 0x555b860f3479 in ?? ??:0
#22 0x555b860e9181 in mojo::MessageDispatcher::Accept(mojo::Message*)
./././mojo/public/cpp/bindings/lib/message_dispatcher.cc:43
#23 0x555b860e9181 in ?? ??:0
#24 0x555b860d08f7 in mojo::Connector::DispatchMessage(mojo::Message)
./././mojo/public/cpp/bindings/lib/connector.cc:546
#25 0x555b860d08f7 in ?? ??:0
#26 0x555b860d2640 in mojo::Connector::ReadAllAvailableMessages()
./././mojo/public/cpp/bindings/lib/connector.cc:604
#27 0x555b860d2640 in ?? ??:0
#28 0x555b8613a2fd in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&)
./././base/callback.h:166
#29 0x555b8613a2fd in OnHandleReady ./././mojo/public/cpp/system/simple_watcher.cc:278
#30 0x555b8613a2fd in ?? ??:0
#31 0x555b8613b2f4 in base::internal::Invoker<base::internal::BindState<void (mojo::SimpleWatcher::*)(int, unsigned int,
mojo::HandleSignalsState const&), base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>,
void (>::RunOnce(base::internal::BindStateBase*) ./././base/bind_internal.h:509
#32 0x555b8613b2f4 in MakeItSo<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &),
base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState> ./././base/bind_internal.h:668
#33 0x555b8613b2f4 in RunImpl<void (mojo::SimpleWatcher::*)(int, unsigned int, const mojo::HandleSignalsState &),
std::__1::tuple<base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>, 0UL, 1UL, 2UL, 3UL>
./././base/bind_internal.h:721
#34 0x555b8613b2f4 in RunOnce ./././base/bind_internal.h:690
#35 0x555b8613b2f4 in ?? ??:0
#36 0x555b8559f070 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./././base/callback.h:98
#37 0x555b8559f070 in RunTask ./././base/task/common/task_annotator.cc:178
#38 0x555b8559f070 in ?? ??:0
#39 0x555b855d8369 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy

```

```

Now*) ../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:360
#40 0x555b855d8369 in ?? ???:0
#41 0x555b855d7ada in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:260
#42 0x555b855d7ada in ?? ???:0
#43 0x555b855d8d11 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc:?
#44 0x555b855d8d11 in ?? ???:0
#45 0x555b8549795f in base::MessagePumpDefault::Run(base::MessagePump::Delegate*)
../../base/message_loop/message_pump_default.cc:39
#46 0x555b8549795f in ?? ???:0
#47 0x555b855d93d4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:467
#48 0x555b855d93d4 in ?? ???:0
#49 0x555b8551ad01 in base::RunLoop::Run(base::Location const&) ../../base/run_loop.cc:134
#50 0x555b8551ad01 in ?? ???:0
#51 0x555b994fc542 in content::RendererMain(content::MainFunctionParams const&)
../../content/renderer/renderer_main.cc:265
#52 0x555b994fc542 in ?? ???:0
#53 0x555b8437d494 in content::RunZygote(content::ContentMainDelegate*)
../../content/app/content_main_runner_impl.cc:582
#54 0x555b8437d494 in ?? ???:0
#55 0x555b84381541 in content::ContentMainRunnerImpl::Run(bool) ../../content/app/content_main_runner_impl.cc:973
#56 0x555b84381541 in ?? ???:0
#57 0x555b8437aac7 in content::RunContentProcess(content::ContentMainParams const&,
content::ContentMainRunner*) ../../content/app/content_main.cc:390
#58 0x555b8437aac7 in ?? ???:0
#59 0x555b8437c6e2 in content::ContentMain(content::ContentMainParams const&)
../../content/app/content_main.cc:418
#60 0x555b8437c6e2 in ?? ???:0
#61 0x555b77485ea5 in ChromeMain ../../chrome/app/chrome_main.cc:172
#62 0x555b77485ea5 in ?? ???:0
error: unknown argument '--demangle=True'
#63 0x7fd74fed50b2 in __libc_start_main ???:?
#64 0x7fd74fed50b2 in ?? ???:0

```

Address 0x7e88c0edc2e8 is a wild pointer inside of access range of size 0x00000000000008.

HINT: if you don't care about these errors you may set ASAN_OPTIONS=detect_container_overflow=0.

If you suspect a false positive see also: <https://github.com/google/sanitizers/wiki/AddressSanitizerContainerOverflow>.

SUMMARY: AddressSanitizer: container-overflow (/home/exp11/asan-linux-release/chrome+0x29dbb217)

Shadow bytes around the buggy address:

```

0x0fd1981d3800: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d3810: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d3820: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d3830: 00 f7 00 f7 00 f7 00 00 00 00 00 00 00 f7 f7 f7
0x0fd1981d3840: f7 00 f7 00 f7 00 f7 00 00 00 00 00 00 00 f7 f7
=>0x0fd1981d3850: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 00[fc]f7 f7
0x0fd1981d3860: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 00 00 f7 f7
0x0fd1981d3870: f7 f7 00 f7 00 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d3880: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d3890: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd1981d38a0: f7 f7 f7 f7 f7 f7 f7 00 f7 00 f7 00 00 00

```

Shadow byte legend (one shadow byte represents 8 application bytes):

Addressable: 00

Partially addressable: 01 02 03 04 05 06 07

Heap left redzone: fa

Freed heap region: fd

Stack left redzone: f1

Stack mid redzone: f2

Stack right redzone: f3

Stack after return: f5

Stack use after scope: f8

Global redzone: f9

Global init order: f6

Poisoned by user: f7

Container overflow: fc

Array cookie: ac

Intra object redzone: bb

ASan internal: fe

Left alloca redzone: ca

Right alloca redzone: cb

==1==ABORTING

Did this work before? N/A

Chrome version: 94.0.4595.0 Channel: n/a

OS Version: 20.04

crash.html

1.0 KB [View](#) [Download](#)

main.html

206 bytes [View](#) [Download](#)

testharness.js

151 KB [View](#) [Download](#)

testharnessreport.js

14.2 KB [View](#) [Download](#)

[Comment 1](#) by [sheriffbot](#) on Tue, Aug 10, 2021, 12:51 AM EDT Project Member

Labels: external_security_report

[Comment 2](#) by [wfh@chromium.org](#) on Tue, Aug 10, 2021, 12:55 PM EDT Project Member

Labels: Needs-Feedback

I am unable to reproduce this on 94.0.4595.0 (Developer Build) (64-bit) asan 907428 on Windows x64. Do you have a more minimized test case that does not require the entire test harness framework to be loaded?

[Comment 3](#) by [wfh@chromium.org](#) on Tue, Aug 10, 2021, 1:01 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Owner: tommy@chromium.org

Cc: guidou@chromium.org hbos@chromium.org

Labels: FoundIn-93 Security_Severity-High OS-Chrome OS-Mac OS-Windows

Components: Blink>GetUserMedia

[Comment 4](#) by [sheriffbot](#) on Tue, Aug 10, 2021, 1:04 PM EDT Project Member

Labels: Security_Impact-Beta

[Comment 5](#) by [sheriffbot](#) on Tue, Aug 10, 2021, 1:07 PM EDT Project Member

Labels: -Pri-2 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 6](#) by [wfh@chromium.org](#) on Tue, Aug 10, 2021, 1:34 PM EDT Project Member

Also unable to reproduce this on linux asan 907424

[Comment 7](#) by [wfh@chromium.org](#) on Tue, Aug 10, 2021, 1:34 PM EDT Project Member

Cc: wfh@chromium.org

[Comment 8](#) by [emily...@gmail.com](#) on Wed, Aug 11, 2021, 8:07 AM EDT

[wfh@chromium.org](#)

Hi, try this new one. It doesn't need test js file anymore.

If still can't repro, add one more launch flag,"--use-fake-ui-for-media-stream". This flag allows the repro without any interaction.

Thanks~

[Deleted] **crash.html**

main.html

206 bytes [View](#) [Download](#)

[Comment 9](#) by [emily...@gmail.com](#) on Wed, Aug 11, 2021, 8:09 AM EDT

Sorry, my mistake.

attached new poc.

crash.html

950 bytes [View](#) [Download](#)

[Comment 10](#) by [sheriffbot](#) on Wed, Aug 11, 2021, 12:46 PM EDT Project Member

Labels: M-93 Target-93

Setting milestone and target because of high severity.

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

[Comment 11](#) by [sheriffbot](#) on Wed, Aug 11, 2021, 12:57 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 12 by wfh@chromium.org on Thu, Aug 12, 2021, 2:56 PM EDT Project Member

Owner: guidou@chromium.org

Cc: -guidou@chromium.org tommi@chromium.org

Thank you for the subsequent proof of concept. I am able to reproduce this now on 94.0.4595.0 (Developer Build) (64-bit) asan 907428. I'm assigning to guidou@chromium.org as it looks like they might have last touched this code.

Comment 13 by wfh@chromium.org on Thu, Aug 12, 2021, 5:24 PM EDT Project Member

Labels: -Needs-Feedback

Comment 14 by pbommana@google.com on Sun, Aug 15, 2021, 10:52 PM EDT Project Member

Cc: herre@google.com

Since guido@ is no longer on Chrome Team, cc'ing herre@ as well.

Comment 15 by toprice@chromium.org on Mon, Aug 16, 2021, 4:18 AM EDT Project Member

Owner: toprice@chromium.org

I can make sure this gets looked at. (btw I'm herre@google.com too - renamed account after a name change)

Looks fairly similar to [crbug/1116903](https://crbug.com/1116903) which Guido looked into a year ago. container-overflow reported on the same iteration.

I'm wondering if the list of sources is being concurrently modified during our iteration due to a race somewhere.

Comment 16 by toprice@chromium.org on Mon, Aug 16, 2021, 4:45 AM EDT Project Member

Summary: container-overflow in blink::UserMediaProcessor::DetermineExistingAudioSessionId (was: container-overflow in blink::UserMediaProcessor::DetermineExistingAudioSessionId)

Comment 17 by adetaylor@google.com on Mon, Aug 16, 2021, 3:01 PM EDT Project Member

I've been asked to comment on whether ReleaseBlock-Stable is correct here.

toprice@, do we know if "--enable-experimental-web-platform-features" is necessary to trigger this? Or any other unusual flags? If so, this would be Security_Impact-None, and we can remove ReleaseBlock-Stable.

Comment 18 by adetaylor@google.com on Thu, Aug 19, 2021, 6:06 PM EDT Project Member

Labels: -Security_Impact-Beta -ReleaseBlock-Stable FoundIn-92 Security_Impact-Extended

wfh@ says "I can repro on M92 92.0.4515.0 (Developer Build) (64-bit) rev 885282" so adjusting labels and removing ReleaseBlock.

Comment 19 by toprice@chromium.org on Fri, Aug 20, 2021, 9:13 AM EDT Project Member

Pretty certain this repros without --enable-experimental-web-platform-features, but yes, present on previous stable builds so not a blocker, thanks.

[Comment 20](#) by dominickn@chromium.org on Thu, Sep 2, 2021, 7:26 AM EDT Project Member

Friendly security marshall ping - where are we with the investigation here? :)

[Comment 21](#) by [sheriffbot](#) on Sat, Sep 4, 2021, 12:21 PM EDT Project Member

toprice: Uh oh! This issue still open and hasn't been updated in the last 15 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 22](#) by [sheriffbot](#) on Sat, Sep 18, 2021, 12:21 PM EDT Project Member

toprice: Uh oh! This issue still open and hasn't been updated in the last 29 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 23](#) by [sheriffbot](#) on Wed, Sep 22, 2021, 12:22 PM EDT Project Member

Labels: -M-93 Target-94 M-94

[Comment 24](#) by toprice@chromium.org on Wed, Oct 6, 2021, 7:48 AM EDT Project Member

I've still not managed to repro the original container-overflow error, but the POC does consistently cause a couple of crashes for me, either:

- FATAL:media_stream_device_observer.cc(238)] Check failed: device_found.

or

-FATAL:user_media_processor.cc(570)] Check failed: !current_request_info_ && !request_completed_cb_ && !local_sources_.size()

Both of these seem to be due to races around user_media_processor, particularly in local_sources_ being added to via a call to eg OnAudioSourceStarted() after StopAllProcessing() has been called but before the object is destroyed.

[Comment 25](#) by emily...@gmail.com on Wed, Oct 6, 2021, 8:09 AM EDT

It is still easy to repro in the new version (Version 96.0.4663.0 (Developer Build) (64-bit) [gs://chromium-browser-asan/linux-release/asan-linux-release-928534.zip](https://chromium-browser-asan/linux-release/asan-linux-release-928534.zip)).

Please check if the following startup switch flags are all enabled?

```
./chrome --user-data-dir=/tmp/xx --incognito --use-fake--for-media-stream --use-fake-device-for-media-stream --enable-experimental-web-platform-features --use-fake-ui-for-media-stream http://localhost:8000/main.html
```

main.html

208 bytes [View](#) [Download](#)

crash2.html

950 bytes [View](#) [Download](#)

[Comment 26](#) by [toprice@chromium.org](#) on Thu, Oct 7, 2021, 8:57 AM EDT Project Member

Ah, yes, with DCHECKs disabled I get the container-overflow repro, that makes sense.

[Comment 27](#) by [sheriffbot](#) on Sat, Oct 9, 2021, 1:45 PM EDT Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

[Comment 28](#) by [adetaylor@google.com](#) on Thu, Nov 11, 2021, 2:17 PM EST Project Member

Cc: [adetaylor@chromium.org](#) [toprice@chromium.org](#)

~~[Issue 1267693](#)~~ has been merged into this issue.

[Comment 29](#) by [adetaylor@google.com](#) on Thu, Nov 11, 2021, 2:17 PM EST Project Member

This bug was resubmitted as ~~[issue 1267693](#)~~, which might have more up-to-date reproduction instructions.

[Comment 30](#) by [sheriffbot](#) on Mon, Nov 15, 2021, 12:22 PM EST Project Member

Labels: -M-94 Target-96 M-96

[Comment 31](#) by [adetaylor@google.com](#) on Mon, Dec 6, 2021, 11:45 AM EST Project Member

[toprice@](#) per e-mail, this is one of our oldest high-sev bugs - and it sounds like you've reproduced it - could you get a CL up this week if possible? If you're blocked on something, please let us know so we can see what we can do to help. Cheers!

[Comment 32](#) by [toprice@chromium.org](#) on Tue, Dec 7, 2021, 5:48 AM EST Project Member

Status: Started (was: Assigned)

Thanks, hoping back on this, hoping to make some progress in the next couple of days (or find someone who can)

[Comment 33](#) by [toprice@chromium.org](#) on Tue, Dec 7, 2021, 9:16 AM EST Project Member

*hopping back on

The issue comes from `UserMediaProcessor::local_sources_` being modified while being iterated over in

UserMediaProcessor::DetermineExistingAudioSessionId().

The weird thing is that it's protected by a `thread_checker_` and the loop doesn't call anything else - it's actually an allocation (caused by `push_back()` on a `HeapVector`), triggering a GC, which garbage collects a `MediaStreamVideoTrack`, whose destructor removes the track from the `MediaStreamSource`, which realises it no longer has tracks, stops itself and calls `UserMediaProcessor::OnLocalSourceStopped` which removes the source from `local_sources_`.

Full symbolised stack trace attached.

So, this pattern of propagating the track removal during destruction means that state can be modified due to GCs pretty much anywhere, and thread checks can't keep things safe.

I'll do something like take a defensive copy of `local_sources_` before doing this loop to solve this case, but for the future we need to work out a better pattern to make these bugs harder to write and make it possible to rely on just `thread_checkers_` to avoid concurrent state modifications.

symbolised_stack.txt

54.1 KB [View](#) [Download](#)

[Comment 34](#) by [adetaylor@chromium.org](#) on Tue, Dec 7, 2021, 10:13 AM EST Project Member

Cc: [danakj@chromium.org](#) [dcheng@chromium.org](#)

+danakj@ and +dcheng@ in case they have thoughts about how this general pattern can be prevented (see [#c33](#))

[Comment 35](#) by [Git Watcher](#) on Fri, Dec 10, 2021, 6:59 AM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+fb6232ffb1fec14d64ec8815f7dfc2cea0887588>

commit [fb6232ffb1fec14d64ec8815f7dfc2cea0887588](#)

Author: Tony Herre <[toprice@chromium.org](#)>

Date: Fri Dec 10 11:58:29 2021

Take local copy of `UMP::local_sources` to iterate

Take a local copy of `UserMediaProcessor::local_sources_` when iterating over it in `UserMediaProcessor::DetermineExistingAudioSessionId`, as the list can be effectively concurrently modified during destruction of `MediaStreamTracks` triggered by GC during this loop. Without the copy this leads to a container overflow.

[Bug-1238209](#)

Change-Id: [I048387a51a58eacff87d220e6b67d2d09f610c1d](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3320283>

Reviewed-by: Henrik Boström <[hbos@chromium.org](#)>

Commit-Queue: Tony Herre <[toprice@chromium.org](#)>

Cr-Commit-Position: refs/heads/main@{#950499}

[modify]

https://crrev.com/fb6232ffb1fec14d64ec8815f7dfc2cea0887588/third_party/blink/renderer/modules/mediastream/user_media_processor.cc

[Comment 36](#) by [herre@google.com](#) on Fri, Dec 10, 2021, 7:40 AM EST Project Member

Labels: Merge-Request-98 Merge-Request-97

[Comment 37](#) by [toprice@chromium.org](#) on Fri, Dec 10, 2021, 9:43 AM EST Project Member

This could be considered closed, as the above cl means we don't hit the container-overflow any more. I want to leave it open a few more days to get some input on safer fixes to this code pattern as mentioned in #33.

danakj@ and dcheng@, anyone else on CC, any thoughts?

[Comment 38](#) by [danakj@chromium.org](#) on Fri, Dec 10, 2021, 9:53 AM EST Project Member

IIUC the problem here is side effects during GC due to putting code in a destructor?

I think destructors + GC continue to be problematic and this is another good example.

Which destructor is causing this data race?

TBC it's running on the same thread, right? But inside push_back()?

[Comment 39](#) by [adetaylor@chromium.org](#) on Fri, Dec 10, 2021, 2:55 PM EST Project Member

Labels: Merge-Request-96

Mustn't forget extended stable (that's one of the reasons we like to allow sheriffbot to add merge requests once bugs are marked fixed)

[Comment 40](#) by [sheriffbot](#) on Sat, Dec 11, 2021, 6:59 AM EST Project Member

Labels: -Merge-Request-98 Hotlist-Merge-Approved Merge-Approved-98

Merge approved: your change passed merge requirements and is auto-approved for M98. Please go ahead and merge the CL to branch 4758 (refs/branch-heads/4758) manually. Please contact milestone owner if you have questions.

Merge instructions:

https://chromium.googlesource.com/chromium/src.git/+refs/heads/main/docs/process/merge_request.md

Owners: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

[Comment 41](#) by [sheriffbot](#) on Sat, Dec 11, 2021, 6:59 AM EST Project Member

Labels: -Merge-Request-97 Hotlist-Merge-Review Merge-Review-97

Merge review required: M97 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:

1. Why does your merge fit within the merge criteria for these milestones?
 - Chrome Browser: <https://chromiumdash.appspot.com/branches>
 - Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
<https://goto.google.com/cros-engprodcomponents>
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.

Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

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

Comment 42 by [sheriffbot](#) on Sat, Dec 11, 2021, 6:59 AM EST Project Member

Labels: -Merge-Request-96 Merge-Review-96

Merge review required: M96 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:

1. Why does your merge fit within the merge criteria for these milestones?
 - Chrome Browser: <https://chromiumdash.appspot.com/branches>
 - Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
<https://goto.google.com/cros-engprodcomponents>
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.

Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 43 by [toprice@chromium.org](#) on Mon, Dec 13, 2021, 5:03 AM EST Project Member

Forking the discussion on lifecycle management to crbug.com/1279340 - danakj@ replied to #38 there.

("allow sheriffbot to add merge requests once bugs are marked fixed" - nice! Didn't know the automation could do that!)

I'll close this to indicate this specific repro should be fixed and track the back merges here.

Comment 44 by [toprice@chromium.org](#) on Mon, Dec 13, 2021, 5:05 AM EST Project Member

Status: Fixed (was: Started)

1. Why does your merge fit within the merge criteria for these milestones?
Severity-High security bug
2. What changes specifically would you like to merge? Please link to Gerrit.
<https://chromium-review.googlesource.com/c/chromium/src/+3320283>
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
No
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
<https://goto.google.com/cros-engprodcomponents>
No
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.
Yes - repro steps in #25

Comment 45 by [sheriffbot](#) on Mon, Dec 13, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 46 by [adetaylor@google.com](#) on Mon, Dec 13, 2021, 1:11 PM EST Project Member

Labels: -Merge-Review-96 -Merge-Review-97 Merge-Approved-96 Merge-Approved-97

Approving merge to M96 (branch 4664), M97 (branch 4692) and M98 (branch 4758). Please go ahead and merge, assuming no problems have shown up in Canary.

Comment 47 by [sheriffbot](#) on Mon, Dec 13, 2021, 1:41 PM EST Project Member

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

Comment 48 by [toprice@chromium.org](#) on Tue, Dec 14, 2021, 3:37 AM EST Project Member

Looking good on Canary. Branch merges in flight: [crrev.com/c/3336878](#), [crrev.com/c/3337259](#), [crrev.com/c/3337896](#)

Comment 49 by [Git Watcher](#) on Tue, Dec 14, 2021, 9:16 AM EST Project Member

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+b54b3361b4b89e711e11f2053d7387a236090253>

commit [b54b3361b4b89e711e11f2053d7387a236090253](#)

Author: Tony Herre <[toprice@chromium.org](#)>

Date: Tue Dec 14 14:15:35 2021

[97] Take local copy of UMP::local_sources to iterate

Take a local copy of UserMediaProcessor::local_sources_ when iterating over it in UserMediaProcessor::DetermineExistingAudioSessionId, as the list can be effectively concurrently modified during destruction of MediaStreamTracks triggered by GC during this loop. Without the copy this leads to a container overflow.

(cherry picked from commit [fb6232ffb1fec14d64ec8815f7dfc2cea0887588](#))

~~Bug-1238209~~

Change-Id: I048387a51a58eacff87d220e6b67d2d09f610c1d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3320283>

Reviewed-by: Henrik Boström <[hbos@chromium.org](#)>

Commit-Queue: Tony Herre <[toprice@chromium.org](#)>

Cr-Original-Commit-Position: refs/heads/main@{#950499}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3337259>

Reviewed-by: Guido Urdaneta <[guidou@chromium.org](#)>

Cr-Commit-Position: refs/branch-heads/4692@{#972}

Cr-Branched-From: [038cd96142d384c0d2238973f1cb277725a62eba](#)-refs/heads/main@{#938553}

[modify]

https://crrev.com/b54b3361b4b89e711e11f2053d7387a236090253/third_party/blink/renderer/modules/mediastream/user_media_processor.cc

Comment 50 by [Git Watcher](#) on Tue, Dec 14, 2021, 11:36 AM EST Project Member

Labels: -merge-approved-96 merge-merged-4664 merge-merged-96

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+5c41beab69428d8c3967cb12d31f921761b85fb4>

commit [5c41beab69428d8c3967cb12d31f921761b85fb4](#)

Author: Tony Herre <toprice@chromium.org>

Date: Tue Dec 14 16:35:05 2021

[96] Take local copy of UMP::local_sources to iterate

Take a local copy of UserMediaProcessor::local_sources_ when iterating over it in UserMediaProcessor::DetermineExistingAudioSessionId, as the list can be effectively concurrently modified during destruction of MediaStreamTracks triggered by GC during this loop. Without the copy this leads to a container overflow.

(cherry picked from commit [fb6232ffb1fec14d64ec8815f7dfc2cea0887588](#))

Bug: [1238209](#)

Change-Id: I048387a51a58eacff87d220e6b67d2d09f610c1d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3320283>

Reviewed-by: Henrik Boström <hbos@chromium.org>

Commit-Queue: Tony Herre <toprice@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#950499}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3337896>

Reviewed-by: Guido Urdaneta <guidou@chromium.org>

Cr-Commit-Position: refs/branch-heads/4664@{#1303}

Cr-Branched-From: [24dc4ee75e01a29d390d43c9c264372a169273a7](#)-refs/heads/main@{#929512}

[modify]

https://crrev.com/5c41beab69428d8c3967cb12d31f921761b85fb4/third_party/blink/renderer/modules/mediastream/user_media_processor.cc

Comment 51 by srinivassista@google.com on Tue, Dec 14, 2021, 1:14 PM EST Project Member

This issue has been approved for Merge to M98, we are cutting the RC build tomorrow for dev release (this will be last release before holidays so please help complete your merge before EOD dec 14, so we can include in dev release.

Comment 52 by [Git Watcher](#) on Tue, Dec 14, 2021, 4:18 PM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+d2bdf6fe2f821da478728b219b38cfb81843e63d>

commit [d2bdf6fe2f821da478728b219b38cfb81843e63d](#)

Author: Tony Herre <toprice@chromium.org>

Date: Tue Dec 14 21:17:06 2021

[98] Take local copy of UMP::local_sources to iterate

Take a local copy of UserMediaProcessor::local_sources_ when iterating over it in UserMediaProcessor::DetermineExistingAudioSessionId, as the list can be effectively concurrently modified during destruction of

MediaStreamTracks triggered by GC during this loop. Without the copy this leads to a container overflow.

(cherry picked from commit [fb6232ffb1fec14d64ec8815f7dfc2cea0887588](#))

~~Bug-1238209~~

Change-Id: I048387a51a58eacff87d220e6b67d2d09f610c1d

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3320283>

Reviewed-by: Henrik Boström <hbos@chromium.org>

Commit-Queue: Tony Herre <toprice@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#950499}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3336878>

Reviewed-by: Guido Urdaneta <guidou@chromium.org>

Cr-Commit-Position: refs/branch-heads/4758@{#43}

Cr-Branched-From: [4a2cf4baf90326df19c3ee70ff987960d59a386e](#)-refs/heads/main@{#950365}

[modify]

https://crrev.com/d2bdf6fe2f821da478728b219b38cfb81843e63d/third_party/blink/renderer/modules/mediastream/user_media_processor.cc

Comment 53 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:32 PM EST Project Member

Labels: Release-0-M97

Comment 54 by amyressler@google.com on Tue, Jan 4, 2022, 1:33 PM EST Project Member

Labels: CVE-2022-0100 CVE_description-missing

Comment 55 by amyressler@google.com on Thu, Feb 17, 2022, 6:34 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** 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 56 by amyressler@chromium.org on Thu, Feb 17, 2022, 6:42 PM EST Project Member

Congratulations! The VRP Panel has decided to award you \$5000 for this report. Thanks for your efforts and nice work!

Comment 57 by amyressler@google.com on Fri, Feb 18, 2022, 2:49 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 58 by [sheriffbot](#) on Mon, Mar 21, 2022, 1:30 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 59](#) by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[About Monorail](#)

[User Guide](#)

[Release Notes](#)

[Feedback on Monorail](#)

[Terms](#)

[Privacy](#)