Talos Vulnerability Report

TALOS-2021-1372

Google Chrome WebRTC RTPSenderVideoFrameTransformerDelegate memory corruption vulnerability

JANUARY 10, 2022

CVE NUMBER

CVE-2021-37979

Summary

A memory corruption vulnerability exists in the WebRTC functionality of Google Chrome 92.0.4515.159 (Stable) and 95.0.4623.0 (Canary). A specially-crafted web page can trigger this vulnerability, which can cause a heap buffer overflow and result in remote code execution. Victim would need to visit a malicious website to trigger this vulnerability.

Tested Versions

Google Chrome 95.0.4623.0 (Canary)
Google Chrome 92.0.4515.159 (Stable)

Product URLs

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

CVSSv3 Score

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

CWE

CWE-122 - Heap-based Buffer Overflow

Details

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

This vulnerability is in WebRTC, which is a technology that enables websites to capture/stream audio/video and other data between browsers.

While executing the attached PoC on Ubuntu 20.04 x64 / Windows 10 x64 machine with ASAN enabled, Chrome crashes inside the SendVideo function from RTPSenderVideoFrameTransformerDelegate. Snippet of this function is as follows:

```
1:  void RTPSenderVideoFrameTransformerDelegate::SendVideo(
2:      std::unique_ptr<TransformableFrameInterface> transformed_frame) const {
3:    RTC_CHECK(encoder_queue_->IsCurrent());
4:    MutexLock lock(&sender_lock_);
5:    if (!sender_)
6:      return;
7:    auto* transformed_video_frame =
8:        static_cast<TransformableVideoSenderFrame*>(transformed_frame.get());
9:    sender_->SendVideo(
10:        transformed_video_frame->GetPayloadType(),
11:        transformed_video_frame->GetCodecType(),
12:        transformed_video_frame->GetTimestamp(),
13:        transformed_video_frame->GetCaptureTimeMs(),
14:        transformed_video_frame->GetData(),
15:        transformed_video_frame->GetHeader(),
16:        transformed_video_frame->GetExpectedRetransmissionTimeMs());
17:  }
```

Based on the contents of the ASAN crash log, crash occurs on line 9. WebRTC is based on two-way communication, and during the initialization phase of WebRTC we need to have a Caller and Callee and create a Reader/Writer relationship for them.

The events required to trigger this vulnerability are convoluted and are best described step by step through javascript code. 1) The PoC creates “ReadableStream.getReader()” which is responsible for reading and locking the stream. 2) A Promise for reading data is created. The expectation is that code inside the Promise should only be in read state. 3) However, inside this Promise the PoC can actually write data using the `WritableStream.getWriter()` object. This results in data that should be read being sent back into the stream with write. 4) After finishing reading the loop (in which the read is actually written), PoC uses custom function `exchangeIceCandidates`, which is a helper function, to exchange ICE candidates between two local peer connections. 5) Last step is to read messeage from sender and write it. However, due to function “exchangeIceCandidates” we are back to point 3.

This results in confusing Callee with Caller, which results in a heap overflow due to constant read and writing of the same data.

With more experimentation with a modified PoC , we can show the following crash:

```
    for (let i = 0; i < 5; i++) {
        const result = await senderReader.read();
        senderWriter.write(result.value);
        result.value.toString()   <-  AddressSanitizer: access-violation on unknown address 0x000000000010
    }
```

Execution crashes because of a NULL pointer de-reference when accessing the object inside loop . This indicates that the object is deleted ahead of time inside the Promise.

The next step in analyzing this issue was to try to create an object that equal to `result`, which contains an object of `ArrayBuffer` type in dictionary `result.value.data`. If there are any expression statements that keep a reference to this data (for example `var x = new DataView(result.value.data)`) then the crash null pointer de-reference doesn't happen. ArrayBuffer object will still be alive and with reference. Keep ArrayBuffer alive like this:

```
for(let i=0;i < 5; i++) {
    const result = awaitt senderReader.read();
     var x = new DataView(result.value.data)
     senderWriter.write(result.value);
     result.value.toString()   <— Does not result in null pointer dereference because result.value.data is retained
 }
```

This would suggest a use-after-free style component to this issue. Therefore, with proper manipulation of streamed data (ArrayBuffer) inside Promise, this vulnerability could lead to further memory corruption and ultimately arbitrary code execution.

Crash Information

```
Steps to reproduce:
a) Without user interaction
chrome.exe --no-sandbox --use-fake-ui-for-media-stream poc.html
b) Clicking allow webcam popup
chrome.exe --no-sandbox poc.html

=================================================================
==20772==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x125a0c2c1ad0 at pc 0x7ff6bae168af bp 0x00809abfe550 sp 0x00809abfe598
READ of size 24 at 0x125a0c2c1ad0 thread T22
==20772==WARNING: Failed to use and restart external symbolizer!
==20772==*** WARNING: Failed to initialize DbgHelp!              ***
==20772==*** Most likely this means that the app is already      ***
==20772==*** using DbgHelp, possibly with incompatible flags.    ***
==20772==*** Due to technical reasons, symbolization might crash ***
==20772==*** or produce wrong results.                           ***
    #0 0x7ff6bae168ae in __asan_memcpy C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_interceptors_memintrinsics.cpp:22
    #1 0x7ffc2f8ce464 in webrtc::RTPSenderVideoFrameTransformerDelegate::SendVideo
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\modules\rtp_rtcp\source\rtp_sender_video_frame_transformer_delegate.cc:159
    #2 0x7ffc2f8cf2bb in webrtc::webrtc_new_closure_impl::ClosureTask<`lambda at
../../third_party/webrtc/modules/rtp_rtcp/source/rtp_sender_video_frame_transformer_delegate.cc:139:7'>::Run
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\rtc_base\task_utils\to_queued_task.h:32
    #3 0x7ffc14d117ec in `anonymous namespace'::WebrtcTaskQueue::RunTask
C:\b\s\w\ir\cache\builder\src\third_party\webrtc_overrides\task_queue_factory.cc:80
    #4 0x7ffc14d11af2 in base::internal::Invoker<base::internal::BindState<void (*)((anonymous namespace)::WebrtcTaskQueue *,
scoped_refptr<base::RefCountedData<bool> >, std::__1::unique_ptr<webrtc::QueuedTask,std::__1::default_delete<webrtc::QueuedTask>
>),base::internal::UnretainedWrapper<(anonymous namespace)::WebrtcTaskQueue>,scoped_refptr<base::RefCountedData<bool>
>,std::__1::unique_ptr<webrtc::QueuedTask,std::__1::default_delete<webrtc::QueuedTask> > >,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #5 0x7ffc1d811bda in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:178
    #6 0x7ffc23864996 in base::internal::TaskTracker::RunSkipOnShutdown
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\task_tracker.cc:663
    #7 0x7ffc2386391e in base::internal::TaskTracker::RunTask C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\task_tracker.cc:524
    #8 0x7ffc23862c6a in base::internal::TaskTracker::RunAndPopNextTask
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\task_tracker.cc:431
    #9 0x7ffc27cf5d34 in base::internal::WorkerThread::RunWorker C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:371
    #10 0x7ffc27cf4e3b in base::internal::WorkerThread::RunPooledWorker
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:262
    #11 0x7ffc1d8d991f in base::`anonymous namespace'::ThreadFunc C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:121
    #12 0x7ff6bae22373 in __asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:278
    #13 0x7ffd34087033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #14 0x7ffd341c2650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

0x125a0c2c1ad0 is located 1968 bytes to the right of 160-byte region [0x125a0c2c1280,0x125a0c2c1320)
allocated by thread T19 here:
    #0 0x7ff6bae16edb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffc2fd50a2a in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffc2f7fe80c in webrtc::RtpVideoStreamReceiverFrameTransformerDelegate::TransformFrame
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver_frame_transformer_delegate.cc:96
    #3 0x7ffc2f31ce3c in webrtc::RtpVideoStreamReceiver2::OnAssembledFrame
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:854
    #4 0x7ffc2f31b0ea in webrtc::RtpVideoStreamReceiver2::OnInsertedPacket
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:763
    #5 0x7ffc2f318526 in webrtc::RtpVideoStreamReceiver2::OnReceivedPayloadData
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:626
    #6 0x7ffc2f31c1e4 in webrtc::RtpVideoStreamReceiver2::ReceivePacket
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:966
    #7 0x7ffc2f31bc3b in webrtc::RtpVideoStreamReceiver2::OnRecoveredPacket
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:649
    #8 0x7ffc2f7f0789 in webrtc::UlpfecReceiverImpl::ProcessReceivedFec
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\modules\rtp_rtcp\source\ulpfec_receiver_impl.cc:175
    #9 0x7ffc2f31bef1 in webrtc::RtpVideoStreamReceiver2::ReceivePacket
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:951
    #10 0x7ffc2f31c437 in webrtc::RtpVideoStreamReceiver2::OnRtpPacket
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\video\rtp_video_stream_receiver2.cc:660
    #11 0x7ffc2f2bd188 in webrtc::RtpDemuxer::OnRtpPacket C:\b\s\w\ir\cache\builder\src\third_party\webrtc\call\rtp_demuxer.cc:249
    #12 0x7ffc2dcf8278 in webrtc::internal::Call::DeliverRtp C:\b\s\w\ir\cache\builder\src\third_party\webrtc\call\call.cc:1593
    #13 0x7ffc2dcf901c in webrtc::internal::Call::DeliverPacket C:\b\s\w\ir\cache\builder\src\third_party\webrtc\call\call.cc:1615
    #14 0x7ffc2dd7f691 in webrtc::webrtc_new_closure_impl::SafetyClosureTask<`lambda at
../../third_party/webrtc/media/engine/webrtc_video_engine.cc:1720:34'>::Run
C:\b\s\w\ir\cache\builder\src\third_party\webrtc\rtc_base\task_utils\to_queued_task.h:50
    #15 0x7ffc1c1f338f in jingle_glue::JingleThreadWrapper::RunTaskQueueTask C:\b\s\w\ir\cache\builder\src\jingle\glue\thread_wrapper.cc:364
    #16 0x7ffc1c1f4ca2 in base::internal::Invoker<base::internal::BindState<void (jingle_glue::JingleThreadWrapper::*)
(std::__1::unique_ptr<webrtc::QueuedTask,std::__1::default_delete<webrtc::QueuedTask>
>),base::WeakPtr<jingle_glue::JingleThreadWrapper>,std::__1::unique_ptr<webrtc::QueuedTask,std::__1::default_delete<webrtc::QueuedTask> >
>,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #17 0x7ffc1d811bda in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:178
    #18 0x7ffc201aa342 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:360
    #19 0x7ffc201a99a2 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:260
    #20 0x7ffc20183937 in base::MessagePumpDefault::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
    #21 0x7ffc201ab83e in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:467
    #22 0x7ffc1d7944d3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:134
    #23 0x7ffc1d857d29 in base::Thread::Run C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:341
    #24 0x7ffc1d858240 in base::Thread::ThreadMain C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:412
    #25 0x7ffc1d8d991f in base::`anonymous namespace'::ThreadFunc C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:121
    #26 0x7ff6bae22373 in __asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:278
    #27 0x7ffd34087033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)

Thread T22 created by T4 here:
    #0 0x7ff6bae22dd2 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_win.cpp:146
    #1 0x7ffc1d8d8cfe in base::`anonymous namespace'::CreateThreadInternal
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:185
    #2 0x7ffc27cf3d5e in base::internal::WorkerThread::Start C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:109
    #3 0x7ffc2387d0b0 in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::WorkerContainer::ForEachWorker<`lambda at
../../base/task/thread_pool/thread_group_impl.cc:185:37'> C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:153
    #4 0x7ffc2387cbdf in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:185
    #5 0x7ffc238763f8 in base::internal::ThreadGroupImpl::WorkerThreadDelegateImpl::GetWork
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:600
    #6 0x7ffc27cf5c9d in base::internal::WorkerThread::RunWorker C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:354
    #7 0x7ffc27cf4e3b in base::internal::WorkerThread::RunPooledWorker
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:262
    #8 0x7ffc1d8d991f in base::`anonymous namespace'::ThreadFunc C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:121
    #9 0x7ff6bae22373 in __asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:278
    #10 0x7ffd34087033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #11 0x7ffd341c2650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)
```

```
Thread T4 created by T0 here:
    #0 0x7ff6bae22dd2 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_win.cpp:146
    #1 0x7ffc1d8d8cfe in base::`anonymous namespace'::CreateThreadInternal
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:185
    #2 0x7ffc27cf3d5e in base::internal::WorkerThread::Start C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\worker_thread.cc:109
    #3 0x7ffc2387d0b0 in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::WorkerContainer::ForEachWorker<`lambda at
../../base/task/thread_pool/thread_group_impl.cc:185:37'> C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:153
    #4 0x7ffc2387cbdf in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:185
    #5 0x7ffc2387451e in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::~ScopedCommandsExecutor
C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:104
    #6 0x7ffc2387394a in base::internal::ThreadGroupImpl::Start C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_group_impl.cc:429
    #7 0x7ffc201b6545 in base::internal::ThreadPoolImpl::Start C:\b\s\w\ir\cache\builder\src\base\task\thread_pool\thread_pool_impl.cc:231
    #8 0x7ffc1faaa7f2 in content::ChildProcess::ChildProcess C:\b\s\w\ir\cache\builder\src\content\child\child_process.cc:80
    #9 0x7ffc267cdf37 in content::RenderProcess::RenderProcess C:\b\s\w\ir\cache\builder\src\content\renderer\render_process.cc:28
    #10 0x7ffc2290745a in content::RenderProcessImpl::RenderProcessImpl
C:\b\s\w\ir\cache\builder\src\content\renderer\render_process_impl.cc:96
    #11 0x7ffc22908069 in content::RenderProcessImpl::Create C:\b\s\w\ir\cache\builder\src\content\renderer\render_process_impl.cc:295
    #12 0x7ffc1fcc39fa in content::RendererMain C:\b\s\w\ir\cache\builder\src\content\renderer\renderer_main.cc:209
    #13 0x7ffc195fa869 in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:973
    #14 0x7ffc195f7282 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:390
    #15 0x7ffc195f8306 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:418
    #16 0x7ffc131a148c in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:172
    #17 0x7ff6bad75b74 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #18 0x7ff6bad72be8 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #19 0x7ff6bb1659af in __scrt_common_main_seh d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #20 0x7ffd34087033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #21 0x7ffd341c2650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

Thread T19 created by T0 here:
    #0 0x7ff6bae22dd2 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_win.cpp:146
    #1 0x7ffc1d8d8cfe in base::`anonymous namespace'::CreateThreadInternal
C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:185
    #2 0x7ffc1d856f4d in base::Thread::StartWithOptions C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:216
    #3 0x7ffc1d856708 in base::Thread::Start C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:168
    #4 0x7ffc2bd2f5dd in blink::PeerConnectionDependencyFactory::CreatePeerConnectionFactory
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\peer_connection_dependency_factory.cc:391
    #5 0x7ffc2bd2f1ca in blink::PeerConnectionDependencyFactory::GetPcFactory
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\peer_connection_dependency_factory.cc:378
    #6 0x7ffc2bd3445a in blink::PeerConnectionDependencyFactory::CreatePeerConnection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\peer_connection_dependency_factory.cc:585
    #7 0x7ffc2cb1562b in blink::RTCPeerConnectionHandler::Initialize
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\rtc_peer_connection_handler.cc:1185
    #8 0x7ffc2ef89b32 in blink::RTCPeerConnection::RTCPeerConnection
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\rtc_peer_connection.cc:848
    #9 0x7ffc2efb63cf in cppgc::MakeGarbageCollectedTrait<blink::RTCPeerConnection>::Call<blink::ExecutionContext
*&,webrtc::PeerConnectionInterface::RTCConfiguration,bool,bool,bool,blink::MediaConstraints &,blink::ExceptionState &>
C:\b\s\w\ir\cache\builder\src\v8\include\cppgc\allocation.h:174
    #10 0x7ffc2ef88c64 in blink::MakeGarbageCollected<blink::RTCPeerConnection,blink::ExecutionContext
*&,webrtc::PeerConnectionInterface::RTCConfiguration,bool,bool,bool,blink::MediaConstraints &,blink::ExceptionState &>
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\platform\heap\v8_wrapper\heap.h:26
    #11 0x7ffc2ef84ca9 in blink::RTCPeerConnection::Create
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\rtc_peer_connection.cc:737
    #12 0x7ffc2ef88fd1 in blink::RTCPeerConnection::Create
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\rtc_peer_connection.cc:782
    #13 0x7ffc2e3deda5 in blink::`anonymous namespace'::v8_rtc_peer_connection::ConstructorCallback
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\third_party\blink\renderer\bindings\modules\v8\v8_rtc_peer_connection.cc:649
    #14 0x7ffc1978de03 in v8::internal::FunctionCallbackArguments::Call C:\b\s\w\ir\cache\builder\src\v8\src\api\api-arguments-inl.h:152
    #15 0x7ffc19789f9d in v8::internal::`anonymous namespace'::HandleApiCallHelper<1>
C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:112
    #16 0x7ffc197884cb in v8::internal::Builtin_Impl_HandleApiCall C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:138
    #17 0x7ffc1978788e in v8::internal::Builtin_HandleApiCall C:\b\s\w\ir\cache\builder\src\v8\src\builtins\builtins-api.cc:130
    #18 0x7eb5000bdffb  (<unknown module>)

SUMMARY: AddressSanitizer: heap-buffer-overflow C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_interceptors_memintrinsics.cpp:22 in __asan_memcpy
Shadow bytes around the buggy address:
  0x04894dad8300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x04894dad8350: fa fa fa fa fa fa fa fa fa fa[fa]fa fa fa fa fa
  0x04894dad8360: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8370: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8380: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad8390: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x04894dad83a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
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
==20772==ABORTING
```

Timeline

2021-09-07 - Vendor Disclosure

2021-10-14 - Vendor Patched

2022-01-10 - Public Release

CREDIT

Discovered by Marcin Towalski of Cisco Talos.