Starred by 7 users

Owner:	hta@chromium.org
CC:	steveanton@chromium.org amyressler@google.com adetaylor@chromium.org mpdenton@chromium.org benmason@chromium.org hta@chromium.org pbomm...@chromium.org natashenka@google.com
Status:	Fixed *(Closed)*
Components:	Blink>WebRTC>PeerConnection
Modified:	Jan 5, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-02-19
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
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-2021-21162

Issue 1172054: UaF in WebRTC P2PSocketManagerProxy::CreateSocket

Reported by emily...@gmail.com on Thu, Jan 28, 2021, 9:48 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36

Steps to reproduce the problem:
Ubuntu 20.04
Chromium 90.0.4400.8 ASAN Build
google-chrome http://localhost:8000/crash.html

Because the crash occurs when the browser is closed, there is only one chance each time.
In my local test, it can be reproduced every 2 or 3 times.

What is the expected behavior?

What went wrong?
==1==ERROR: AddressSanitizer: heap-use-after-free on address 0x60b00003efd0 at pc 0x55c04e235a38 bp 0x7fa067e059f0 sp 0x7fa067e059e8
READ of size 8 at 0x60b00003efd0 thread T15 (WebRTC_Network)
    #0 0x55c04e235a37 in network::mojom::blink::P2PSocketManagerProxy::CreateSocket(network::P2PSocketType, net::IPEndPoint const&, network::P2PPortRange const&, network::P2PHostAndIPEndPoint const&, mojo::PendingRemote<network::mojom::blink::P2PSocketClient>, mojo::PendingReceiver<network::mojom::blink::P2PSocket>) ./gen/services/network/public/mojom/p2p.mojom-blink.cc:414:17
    #1 0x55c063c1ba3c in blink::P2PSocketClientImpl::Init(network::P2PSocketType, net::IPEndPoint const&, unsigned short, unsigned short, network::P2PHostAndIPEndPoint const&, blink::P2PSocketClientDelegate*) ./../../third_party/blink/renderer/platform/p2p/socket_client_impl.cc:59:39
    #2 0x55c063c14f28 in blink::(anonymous namespace)::IpcPacketSocket::Init(network::P2PSocketType, std::__1::unique_ptr<blink::P2PSocketClientImpl, std::__1::default_delete<blink::P2PSocketClientImpl> >, rtc::SocketAddress const&, unsigned short, unsigned short, rtc::SocketAddress const&) ./../../third_party/blink/renderer/platform/p2p/ipc_socket_factory.cc:319:15
    #3 0x55c063c14939 in blink::IpcPacketSocketFactory::CreateUdpSocket(rtc::SocketAddress const&, unsigned short, unsigned short) ./../../third_party/blink/renderer/platform/p2p/ipc_socket_factory.cc:729:16
    #4 0x55c063b9f0e0 in cricket::AllocationSequence::Init() ./../../third_party/webrtc/p2p/client/basic_port_allocator.cc:1237:51
    #5 0x55c063b9a5ad in cricket::BasicPortAllocatorSession::DoAllocate(bool) ./../../third_party/webrtc/p2p/client/basic_port_allocator.cc:820:17
    #6 0x55c063b93b05 in cricket::BasicPortAllocatorSession::OnNetworksChanged() ./../../third_party/webrtc/p2p/client/basic_port_allocator.cc:857:5
    #7 0x55c063c22607 in emit<> ./../../third_party/webrtc/rtc_base/third_party/sigslot/sigslot.h:327:5
    #8 0x55c063c22607 in emit ./../../third_party/webrtc/rtc_base/third_party/sigslot/sigslot.h:560:12
    #9 0x55c063c22607 in operator() ./../../third_party/webrtc/rtc_base/third_party/sigslot/sigslot.h:564:35
    #10 0x55c063c22607 in blink::FilteringNetworkManager::SendNetworksChangedSignal() ./../../third_party/blink/renderer/platform/p2p/filtering_network_manager.cc:216:3
    #11 0x55c063c22bd0 in Invoke<void (blink::FilteringNetworkManager::*)(), base::WeakPtr<blink::FilteringNetworkManager>> ./../../base/bind_internal.h:498:12
    #12 0x55c063c22bd0 in MakeItSo<void (blink::FilteringNetworkManager::*)(), base::WeakPtr<blink::FilteringNetworkManager>> ./../../base/bind_internal.h:657:5
    #13 0x55c063c22bd0 in RunImpl<void (blink::FilteringNetworkManager::*)(), std::tuple<base::WeakPtr<blink::FilteringNetworkManager> >, 0> ./../../base/bind_internal.h:710:12
    #14 0x55c063c22bd0 in base::internal::Invoker<base::internal::BindState<void (blink::FilteringNetworkManager::*)(), base::WeakPtr<blink::FilteringNetworkManager> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:679:12
    #15 0x55c051fc41a3 in Run ./../../base/callback.h:101:12
    #16 0x55c051fc41a3 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:163:33
    #17 0x55c0520040b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #18 0x55c052003870 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36

```
    #19 0x55c051ec0f20 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39:55
    #20 0x55c05200594c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460:12
    #21 0x55c051f4a6ad in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133:14
    #22 0x55c05205d392 in base::Thread::Run(base::RunLoop*) ./../../base/threading/thread.cc:311:13
    #23 0x55c05205d90f in base::Thread::ThreadMain() ./../../base/threading/thread.cc:382:3
    #24 0x55c0520ed721 in base::(anonymous namespace)::ThreadFunc(void*) ./../../base/threading/platform_thread_posix.cc:87:13
    #25 0x7fa081da9608 in start_thread /build/glibc-eX1tMB/glibc-2.31/nptl/pthread_create.c:477:8

0x60b00003efd0 is located 96 bytes inside of 104-byte region [0x60b00003ef70,0x60b00003efd8)
freed by thread T0 (swain) here:
    #0 0x55c0458c2ded in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x55c063c060c9 in operator() ./../../buildtools/third_party/libc++/trunk/include/memory:2378:5
    #2 0x55c063c060c9 in reset ./../../buildtools/third_party/libc++/trunk/include/memory:2633:7
    #3 0x55c063c060c9 in ~unique_ptr ./../../buildtools/third_party/libc++/trunk/include/memory:2587:19
    #4 0x55c063c060c9 in ~SharedRemoteBase ./../../mojo/public/cpp/bindings/shared_remote.h:205:24
    #5 0x55c063c060c9 in DeleteInternal<mojo::SharedRemoteBase<mojo::Remote<network::mojom::blink::P2PSocketManager> > > ./../../base/memory/ref_counted.h:412:5
    #6 0x55c063c060c9 in Destruct ./../../base/memory/ref_counted.h:367:5
    #7 0x55c063c060c9 in Release ./../../base/memory/ref_counted.h:401:7
    #8 0x55c063c060c9 in Release ./../../base/memory/scoped_refptr.h:322:8
    #9 0x55c063c060c9 in ~scoped_refptr ./../../base/memory/scoped_refptr.h:224:7
    #10 0x55c063c060c9 in reset ./../../base/memory/scoped_refptr.h:254:18
    #11 0x55c063c060c9 in reset ./../../mojo/public/cpp/bindings/shared_remote.h:273:26
    #12 0x55c063c060c9 in blink::P2PSocketDispatcher::OnConnectionError() ./../../third_party/blink/renderer/platform/p2p/socket_dispatcher.cc:112:23
    #13 0x55c051fc41a3 in Run ./../../base/callback.h:101:12
    #14 0x55c051fc41a3 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:163:33
    #15 0x55c0520040b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #16 0x55c052003870 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #17 0x55c051ec0f20 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39:55
    #18 0x55c052005ae7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:457:12
    #19 0x55c051f4a6ad in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133:14
    #20 0x55c067206fb9 in printing::PrintRenderFrameHelper::RequestPrintPreview(printing::PrintRenderFrameHelper::PrintPreviewRequestType)
./../../components/printing/renderer/print_render_frame_helper.cc:2421:12
    #21 0x55c067205d69 in printing::PrintRenderFrameHelper::ScriptedPrint(bool) ./../../components/printing/renderer/print_render_frame_helper.cc:1161:5
    #22 0x55c064e55585 in content::RenderFrameImpl::ScriptedPrint(bool) ./../../content/renderer/render_frame_impl.cc:2172:14
    #23 0x55c060fb3a9e in blink::ChromeClientImpl::PrintDelegate(blink::LocalFrame*) ./../../third_party/blink/renderer/core/page/chrome_client_impl.cc:569:26
    #24 0x55c060fad33d in blink::ChromeClient::Print(blink::LocalFrame*) ./../../third_party/blink/renderer/core/page/chrome_client.cc:320:3
    #25 0x55c06631c3d9 in blink::(anonymous namespace)::PrintOperationCallback(v8::FunctionCallbackInfo<v8::Value> const&)
./gen/third_party/blink/renderer/bindings/modules/v8/v8_window.cc:19044:19
    #26 0x55c04e943fcc in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./../../v8/src/api/api-arguments-inl.h:158:3
    #27 0x55c04e941a7b in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) ./../../v8/src/builtins/builtins-api.cc:113:36
    #28 0x55c04e93f647 in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) ./../../v8/src/builtins/builtins-api.cc:143:5
    #29 0x55c050b48bf7 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
    #30 0x55c050ae338e in Builtins_InterpreterEntryTrampoline ??:0:0
    #31 0x55c050b4ad12 in Builtins_GetProperty ??:0:0
    #32 0x55c050b9303c in Builtins_ResolvePromise ??:0:0
    #33 0x55c050b8b3cc in Builtins_PromiseCapabilityDefaultResolve ??:0:0
    #34 0x55c050b9283a in Builtins_PromiseFulfillReactionJob ??:0:0
    #35 0x55c050b03136 in Builtins_RunMicrotasks ??:0:0
    #36 0x55c050ae0f77 in Builtins_JSRunMicrotasksEntry ??:0:0
    #37 0x55c04ec04fac in Call ./../../v8/src/execution/simulator.h:142:12
    #38 0x55c04ec04fac in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous namespace)::InvokeParams const&)
./../../v8/src/execution/execution.cc:383:33
    #39 0x55c04ec08a4e in v8::internal::(anonymous namespace)::InvokeWithTryCatch(v8::internal::Isolate*, v8::internal::(anonymous namespace)::InvokeParams const&)
./../../v8/src/execution/execution.cc:428:20
    #40 0x55c04ec08ee9 in v8::internal::Execution::TryRunMicrotasks(v8::internal::Isolate*, v8::internal::MicrotaskQueue*, v8::internal::MaybeHandle<v8::internal::Object>*)
./../../v8/src/execution/execution.cc:505:10
    #41 0x55c04ec96082 in v8::internal::MicrotaskQueue::RunMicrotasks(v8::internal::Isolate*) ./../../v8/src/execution/microtask-queue.cc:165:22
    #42 0x55c04ec95a16 in v8::internal::MicrotaskQueue::PerformCheckpoint(v8::Isolate*) ./../../v8/src/execution/microtask-queue.cc:117:5

previously allocated by thread T0 (swain) here:
    #0 0x55c0458c258d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x55c063c0c215 in make_unique<mojo::ThreadSafeForwarder<network::mojom::blink::P2PSocketManager>, const scoped_refptr<base::SequencedTaskRunner> &,
base::RepeatingCallback<void (mojo::Message)>, base::RepeatingCallback<void (mojo::Message, std::unique_ptr<mojo::MessageReceiver>)>,
base::RepeatingCallback<void (bool)>, mojo::AssociatedGroup &> ./../../buildtools/third_party/libc++/trunk/include/memory:3043:28
    #2 0x55c063c0c215 in mojo::SharedRemoteBase<mojo::Remote<network::mojom::blink::P2PSocketManager> >::RemoteWrapper::CreateForwarder()
./../../mojo/public/cpp/bindings/shared_remote.h:91:14
    #3 0x55c063c0af40 in SharedRemoteBase ./../../mojo/public/cpp/bindings/shared_remote.h:180:60
    #4 0x55c063c0af40 in mojo::SharedRemoteBase<mojo::Remote<network::mojom::blink::P2PSocketManager>
>::Create(mojo::PendingRemote<network::mojom::blink::P2PSocketManager>) ./../../mojo/public/cpp/bindings/shared_remote.h:189:16
    #5 0x55c063c0a5c8 in mojo::SharedRemote<network::mojom::blink::P2PSocketManager>::Bind(mojo::PendingRemote<network::mojom::blink::P2PSocketManager>,
scoped_refptr<base::SequencedTaskRunner>) ./../../mojo/public/cpp/bindings/shared_remote.h:298:17
    #6 0x55c063c05508 in SharedRemote ./../../mojo/public/cpp/bindings/shared_remote.h:239:5
    #7 0x55c063c05508 in blink::P2PSocketDispatcher::GetP2PSocketManager() ./../../third_party/blink/renderer/platform/p2p/socket_dispatcher.cc:48:9
    #8 0x55c063c04df6 in blink::P2PSocketDispatcher::RequestNetworkEventsIfNecessary() ./../../third_party/blink/renderer/platform/p2p/socket_dispatcher.cc:105:5
    #9 0x55c051fc41a3 in Run ./../../base/callback.h:101:12
    #10 0x55c051fc41a3 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:163:33
    #11 0x55c0520040b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #12 0x55c052003870 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #13 0x55c051ec0f20 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39:55
    #14 0x55c05200594c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460:12
    #15 0x55c051f4a6ad in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133:14
    #16 0x55c066f8b8b5 in content::RendererMain(content::MainFunctionParams const&) ./../../content/renderer/renderer_main.cc:260:16
    #17 0x55c051c959c0 in content::RunZygote(content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:534:14
    #18 0x55c051c98e65 in content::ContentMainRunnerImpl::Run(bool) ./../../content/app/content_main_runner_impl.cc:937:10
    #19 0x55c051c92def in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) ./../../content/app/content_main.cc:372:36
    #20 0x55c051c933e8 in content::ContentMain(content::ContentMainParams const&) ./../../content/app/content_main.cc:398:10
    #21 0x55c0458c57e3 in ChromeMain ./../../chrome/app/chrome_main.cc:141:12
    #22 0x7fa07ff380b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

Thread T15 (WebRTC_Network) created by T0 (swain) here:
    #0 0x55c0458822aa in pthread_create /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_interceptors.cpp:214:3
    #1 0x55c0520ec93a in base::(anonymous namespace)::CreateThread(unsigned long, bool, base::PlatformThread::Delegate*, base::PlatformThreadHandle*,
base::ThreadPriority) ./../../base/threading/platform_thread_posix.cc:126:13
    #2 0x55c05205c68f in base::Thread::StartWithOptions(base::Thread::Options const&) ./../../base/threading/thread.cc:186:15
```

```
    #3 0x55c05205c037 in base::Thread::Start() ./../../base/threading/thread.cc:139:10
    #4 0x55c063af3a36 in blink::PeerConnectionDependencyFactory::CreatePeerConnectionFactory()
./../../third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc:219:3
    #5 0x55c063af30c9 in blink::PeerConnectionDependencyFactory::GetPcFactory()
./../../third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc:158:5
    #6 0x55c063af72ba in blink::PeerConnectionDependencyFactory::CreatePeerConnection(webrtc::PeerConnectionInterface::RTCConfiguration const&,
blink::WebLocalFrame*, webrtc::PeerConnectionObserver*, blink::ExceptionState&)
./../../third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc:383:8
    #7 0x55c0649889f4 in blink::RTCPeerConnectionHandler::Initialize(webrtc::PeerConnectionInterface::RTCConfiguration const&, blink::MediaConstraints const&,
blink::WebLocalFrame*, blink::ExceptionState&) ./../../third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc:1183:50
    #8 0x55c0667cf22e in blink::RTCPeerConnection::RTCPeerConnection(blink::ExecutionContext*, webrtc::PeerConnectionInterface::RTCConfiguration, bool, bool, bool,
blink::MediaConstraints, blink::ExceptionState&) ./../../third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc:808:23
    #9 0x55c0667c8659 in Call<blink::ExecutionContext *&, webrtc::PeerConnectionInterface::RTCConfiguration, bool, bool, bool, blink::MediaConstraints &,
blink::ExceptionState &> ./../../third_party/blink/renderer/platform/heap/impl/heap.h:568:32
    #10 0x55c0667c8659 in MakeGarbageCollected<blink::RTCPeerConnection, blink::ExecutionContext *&, webrtc::PeerConnectionInterface::RTCConfiguration, bool, bool,
bool, blink::MediaConstraints &, blink::ExceptionState &> ./../../third_party/blink/renderer/platform/heap/impl/heap.h:608:15
    #11 0x55c0667c8659 in blink::RTCPeerConnection::Create(blink::ExecutionContext*, blink::RTCConfiguration const*, blink::Dictionary const&, blink::ExceptionState&)
./../../third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc:700:40
    #12 0x55c0667ce69d in blink::RTCPeerConnection::Create(blink::ExecutionContext*, blink::RTCConfiguration const*, blink::ExceptionState&)
./../../third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc:738:10
    #13 0x55c0668e10dc in blink::(anonymous namespace)::ConstructorCallback(v8::FunctionCallbackInfo<v8::Value> const&)
./gen/third_party/blink/renderer/bindings/modules/v8/v8_rtc_peer_connection.cc:649:22
    #14 0x55c04e943fcc in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./../../v8/src/api/api-arguments-inl.h:158:3
    #15 0x55c04e940c84 in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<true>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) ./../../v8/src/builtins/builtins-api.cc:113:36
    #16 0x55c04e93f5b6 in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) ./../../v8/src/builtins/builtins-api.cc:139:5
    #17 0x55c050b48bf7 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
    #18 0x55c050ae05e0 in Builtins_JSBuiltinsConstructStub ??:0:0
    #19 0x55c050bd4c47 in Builtins_ConstructHandler ??:0:0
    #20 0x55c050ae338e in Builtins_InterpreterEntryTrampoline ??:0:0
    #21 0x55c050b90e21 in Builtins_PromiseConstructor ??:0:0
    #22 0x55c050ae05e0 in Builtins_JSBuiltinsConstructStub ??:0:0
    #23 0x55c050bd4c47 in Builtins_ConstructHandler ??:0:0
    #24 0x55c050ae338e in Builtins_InterpreterEntryTrampoline ??:0:0
    #25 0x55c050ae338e in Builtins_InterpreterEntryTrampoline ??:0:0
    #26 0x55c050ae101a in Builtins_JSEntryTrampoline ??:0:0
    #27 0x55c050ae0df7 in Builtins_JSEntry ??:0:0
    #28 0x55c04ec051a5 in Call ./../../v8/src/execution/simulator.h:142:12
    #29 0x55c04ec051a5 in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous namespace)::InvokeParams const&)
./../../v8/src/execution/execution.cc:368:33
    #30 0x55c04ec041be in v8::internal::Execution::Call(v8::internal::Isolate*, v8::internal::Handle<v8::internal::Object>, v8::internal::Handle<v8::internal::Object>, int,
v8::internal::Handle<v8::internal::Object>*) ./../../v8/src/execution/execution.cc:462:10
    #31 0x55c04e7caf31 in v8::Script::Run(v8::Local<v8::Context>) ./../../v8/src/api/api.cc:2150:7
    #32 0x55c061b46508 in blink::V8ScriptRunner::RunCompiledScript(v8::Isolate*, v8::Local<v8::Script>, blink::ExecutionContext*)
./../../third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:371:22
    #33 0x55c061b47747 in blink::V8ScriptRunner::CompileAndRunScript(v8::Isolate*, blink::ScriptState*, blink::ExecutionContext*, blink::ScriptSourceCode const&,
blink::KURL const&, blink::SanitizeScriptErrors, blink::ScriptFetchOptions const&, blink::ExecuteScriptPolicy, blink::V8ScriptRunner::RethrowErrorsOption)
./../../third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:462:11
    #34 0x55c061a84c36 in blink::ScriptController::ExecuteScriptAndReturnValue(v8::Local<v8::Context>, blink::ScriptSourceCode const&, blink::KURL const&,
blink::SanitizeScriptErrors, blink::ScriptFetchOptions const&, blink::ExecuteScriptPolicy) ./../../third_party/blink/renderer/bindings/core/v8/script_controller.cc:92:35
    #35 0x55c061a874f6 in blink::ScriptController::EvaluateScriptInMainWorld(blink::ScriptSourceCode const&, blink::KURL const&, blink::SanitizeScriptErrors,
blink::ScriptFetchOptions const&, blink::ExecuteScriptPolicy) ./../../third_party/blink/renderer/bindings/core/v8/script_controller.cc:286:10
    #36 0x55c061400551 in RunScriptAndReturnValue ./../../third_party/blink/renderer/core/script/classic_script.cc:42:40
    #37 0x55c061400551 in RunScript ./../../third_party/blink/renderer/core/script/classic_script.cc:36:3
    #38 0x55c061400551 in blink::ClassicScript::RunScript(blink::LocalDOMWindow*) ./../../third_party/blink/renderer/core/script/classic_script.cc:29:10
    #39 0x55c0614552f3 in blink::PendingScript::ExecuteScriptBlockInternal(blink::Script*, blink::ScriptElementBase*, bool, bool, bool, base::TimeTicks, bool)
./../../third_party/blink/renderer/core/script/pending_script.cc:264:13
    #40 0x55c061454bfd in blink::PendingScript::ExecuteScriptBlock(blink::KURL const&) ./../../third_party/blink/renderer/core/script/pending_script.cc:170:3
    #41 0x55c06144bac6 in blink::ScriptLoader::PrepareScript(WTF::TextPosition const&, blink::ScriptLoader::LegacyTypeSupport)
./../../third_party/blink/renderer/core/script/script_loader.cc:960:9
    #42 0x55c0627a37da in blink::HTMLParserScriptRunner::ProcessScriptElementInternal(blink::Element*, WTF::TextPosition const&)
./../../third_party/blink/renderer/core/script/html_parser_script_runner.cc:609:20
    #43 0x55c0627a3378 in blink::HTMLParserScriptRunner::ProcessScriptElement(blink::Element*, WTF::TextPosition const&)
./../../third_party/blink/renderer/core/script/html_parser_script_runner.cc:332:3
    #44 0x55c062757a72 in blink::HTMLDocumentParser::RunScriptsForPausedTreeBuilder()
./../../third_party/blink/renderer/core/html/parser/html_document_parser.cc:659:21
    #45 0x55c06275b61d in
blink::HTMLDocumentParser::ProcessTokenizedChunkFromBackgroundParser(std::__1::unique_ptr<blink::HTMLDocumentParser::TokenizedChunk,
std::__1::default_delete<blink::HTMLDocumentParser::TokenizedChunk> >, bool*) ./../../third_party/blink/renderer/core/html/parser/html_document_parser.cc:903:9
    #46 0x55c0627572f6 in blink::HTMLDocumentParser::PumpPendingSpeculations() ./../../third_party/blink/renderer/core/html/parser/html_document_parser.cc:963:34
    #47 0x55c062756c7b in blink::HTMLDocumentParser::ResumeParsingAfterYield() ./../../third_party/blink/renderer/core/html/parser/html_document_parser.cc:646:3
    #48 0x55c050c97b61 in Run ./../../base/callback.h:101:12
    #49 0x55c050c97b61 in blink::TaskHandle::Runner::Run(blink::TaskHandle const&)
./../../third_party/blink/renderer/platform/scheduler/common/post_cancellable_task.cc:47:21
    #50 0x55c050c98b22 in Invoke<void (blink::TaskHandle::Runner::*)(const blink::TaskHandle &), base::WeakPtr<blink::TaskHandle::Runner>, blink::TaskHandle>
./../../base/bind_internal.h:498:12
    #51 0x55c050c98b22 in MakeItSo<void (blink::TaskHandle::Runner::*)(const blink::TaskHandle &), base::WeakPtr<blink::TaskHandle::Runner>, blink::TaskHandle>
./../../base/bind_internal.h:657:5
    #52 0x55c050c98b22 in RunImpl<void (blink::TaskHandle::Runner::*)(const blink::TaskHandle &), std::tuple<base::WeakPtr<blink::TaskHandle::Runner>,
blink::TaskHandle>, 0, 1> ./../../base/bind_internal.h:710:12
    #53 0x55c050c98b22 in base::internal::Invoker<base::internal::BindState<void (blink::TaskHandle::Runner::*)(blink::TaskHandle const&),
base::WeakPtr<blink::TaskHandle::Runner>, blink::TaskHandle>, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:679:12
    #54 0x55c051fc41a3 in Run ./../../base/callback.h:101:12
    #55 0x55c051fc41a3 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:163:33
    #56 0x55c0520040b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:351:25
    #57 0x55c052003870 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264:36
    #58 0x55c051ec0f20 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39:55
    #59 0x55c05200594c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460:12
    #60 0x55c051f4a6ad in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133:14
    #61 0x55c066f8b8b5 in content::RendererMain(content::MainFunctionParams const&) ./../../content/renderer/renderer_main.cc:260:16
    #62 0x55c051c959c0 in content::RunZygote(content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:534:14
    #63 0x55c051c98e65 in content::ContentMainRunnerImpl::Run(bool) ./../../content/app/content_main_runner_impl.cc:937:10
    #64 0x55c051c92def in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) ./../../content/app/content_main.cc:372:36
    #65 0x55c051c933e8 in content::ContentMain(content::ContentMainParams const&) ./../../content/app/content_main.cc:398:10
    #66 0x55c0458c57e3 in ChromeMain ./../../chrome/app/chrome_main.cc:141:12
    #67 0x7fa07ff380b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free (/home/pwnexp/chromium/src/out/chrome_asan_shared/swain+0x12e29a37)
Shadow bytes around the buggy address:
```

```
  0x0c167ffffda0: fd fd fd fa fa fa fa fa fa fa fa fd fd fd fd
  0x0c167ffffdb0: fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x0c167ffffdc0: fa fa fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c167ffffdd0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd
  0x0c167ffffde0: fd fd fd fd fd fa fa fa fa fa fa fa fa fd fd
=>0x0c167ffffdf0: fd fd fd fd fd fd fd fd fd fd[fd]fa fa fa fa
  0x0c167ffffe00: fa fa fa fa fd fd fd fd fd fd fd fd fd fd fd
  0x0c167ffffe10: fd fa fa fa fa fa fa fa fa fa fa fd fd fd fd
  0x0c167ffffe20: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c167ffffe30: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa
  0x0c167ffffe40: fa fa fa fa fa fa fd fd fd fd fd fd fd fd fd
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
  Shadow gap:              cc
==1==ABORTING
```

Did this work before? N/A

Chrome version: Chromium 90.0.4400.8 Channel: dev
OS Version: 20.04
Flash Version:

crash.html
369 bytes View Download

Comment 1 by sheriffbot on Thu, Jan 28, 2021, 9:49 PM EST Project Member

Labels: external_security_report

Comment 2 by rsleevi@chromium.org on Fri, Jan 29, 2021, 3:46 PM EST Project Member

Owner: sergeyu@chromium.org
Cc: hta@chromium.org mpdenton@chromium.org
Labels: Security_Severity-High Security_Impact-Stable
Components: Blink>WebRTC>PeerConnection

sergeyu: I've not yet confirmed or reproduced this, so apologies for possible noise, but knowing we previously had some lifetime issues here in this code that you'd worked through (IIRC), I thought it best to pre-emptively CC. Just from reading the code, it does look legit, and from the code analysis, I'm setting the Stable impact.

The P2PSocketManager is managed as a SharedRemote, owned by the P2PSocketDispatcher (which is refcounted). The PeerConnectionDependencyFactory keeps the P2PSocketDispatcher alive, but the P2PSocketDispatcher resets the P2PSocketManager on a Mojo error (https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/p2p/socket_dispatcher.cc;l=110;drc=62ed285cc8715be55d14e614d38fdd61612a9f6b), and needs to be reconnected asynchronously (in case the network service restarted)

The IpcPacketSocketFactory takes a non-owning pointer to the P2PSocketDispatcher in the PeerConnectionDependencyFactory, but the P2PSocketClientImpl unconditionally assumes there will always be a P2PSocketManager (https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/p2p/socket_client_impl.cc;l=59;drc=1d687af38408d6fb1945d5e7a06c9e5215bc8514)

This same issue also seems it would affect the P2PAsyncAddressResolver (https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/p2p/host_address_request.cc;l=37;drc=62ed285cc8715be55d14e614d38fdd61612a9f6b).

This would only trigger on shutdown because it's a race with the network service shutdown, but if someone was able to reliably crash the network service, it seems like they'd be able to reliably exploit this.

CC'ing mpdenton@ as FYI, as I seem to recall we had a similar variant in the CertVerifierService stuff, which I can't remember how we solved :) But I suspect you'll know the lifecycle better to know how you want to manage the state machine when the network service is restarting.

Comment 3 by rsleevi@chromium.org on Fri, Jan 29, 2021, 7:20 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 4 by sheriffbot on Sat, Jan 30, 2021, 12:47 PM EST Project Member

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 5 by sheriffbot on Sat, Jan 30, 2021, 1:27 PM EST 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 rsleevi@chromium.org on Mon, Feb 1, 2021, 3:23 PM EST Project Member

Labels: OS-Android OS-Chrome OS-Mac OS-Windows

Comment 7 by ClusterFuzz on Thu, Feb 11, 2021, 4:50 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5650175927058432.

Comment 8 by rsesek@chromium.org on Thu, Feb 11, 2021, 5:28 PM EST Project Member

Summary: UaF in WebRTC P2PSocketManagerProxy::CreateSocket (was: uaf in webrtc)
Owner: guidou@chromium.org
Cc: steveanton@chromium.org

guidou: Can you take a look at this?

Comment 9 by mpdenton@chromium.org on Thu, Feb 11, 2021, 6:40 PM EST Project Member

Seems like a race condition between the two threads.

OnConnectionError(), which runs on the main thread, does take a lock before resetting the p2p_socket_manager_, a SharedRemote:

```
void P2PSocketDispatcher::OnConnectionError() {
  base::AutoLock lock(p2p_socket_manager_lock_);
  p2p_socket_manager_.reset();
  // ...
}
```

And GetP2PSocketManager(), which runs on the "peer connection networking thread" does take the lock as well.

```
network::mojom::blink::P2PSocketManager*
P2PSocketDispatcher::GetP2PSocketManager() {
  base::AutoLock lock(p2p_socket_manager_lock_);
  // ...
  return p2p_socket_manager_.get();
}
```

But it doesn't matter:

```
void P2PSocketClientImpl::Init(...) {
  // ...
  dispatcher_->GetP2PSocketManager()->CreateSocket(
      type, local_address, network::P2PPortRange(min_port, max_port),
      remote_address, receiver_.BindNewPipeAndPassRemote(),
      socket_.BindNewPipeAndPassReceiver());
  // ...
}
```

P2PSocketClientImpl::Init() uses the raw pointer returned by GetP2PSocketManager without holding a reference to the SharedRemote and without holding the lock that protects the shared remote, so the P2PSocketManager just gets deleted on the main thread during OnConnectionError(), while P2PSocketClientImpl::Init() is using it.

Comment 10 by mpdenton@chromium.org on Thu, Feb 11, 2021, 6:46 PM EST Project Member

Looks like sergeyu@ noticed this issue previously here https://chromium-review.googlesource.com/c/chromium/src/+/1260363/comment/32c27608_bbbef367/ and a scoped_refptr was used, but it got switched back to a raw pointer in a refactor (https://chromium-review.googlesource.com/c/chromium/src/+/1924331)

Comment 11 by mpdenton@chromium.org on Thu, Feb 11, 2021, 6:48 PM EST Project Member

rsleevi@: this is unrelated to my issue with the CertVerifierService, since I only needed a Remote<> and therefore I could use a raw pointer without worrying that the connection's error handler would reset my Remote<> on another thread. Here, the raw pointer is to a SharedRemote, which can in fact by reset on another thread.

Comment 12 by sheriffbot on Fri, Feb 12, 2021, 12:21 PM EST Project Member

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

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

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

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

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

Comment 13 by hta@chromium.org on Sun, Feb 14, 2021, 5:09 AM EST Project Member

Owner: hta@chromium.org

I think I have a fix.

Comment 14 by bugdroid on Mon, Feb 15, 2021, 10:50 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/82cdc0781ceb4c22ef5903cf3115bea518a5523b

commit 82cdc0781ceb4c22ef5903cf3115bea518a5523b
Author: Harald Alvestrand <hta@chromium.org>
Date: Mon Feb 15 15:49:49 2021

Fix GetP2PSocketManager ownership

Let it return a mojo::SharedRemote<> instead of a raw pointer - this is
a decoration around a shared_refptr.

~~Bug: chromium:1172054~~
Change-Id: I49bd22a0dc949bf869744d2ad25c1afcaea7fdbc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2692532
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Commit-Position: refs/heads/master@{#854050}

[modify] https://crrev.com/82cdc0781ceb4c22ef5903cf3115bea518a5523b/third_party/blink/renderer/platform/p2p/socket_dispatcher.h
[modify] https://crrev.com/82cdc0781ceb4c22ef5903cf3115bea518a5523b/third_party/blink/renderer/platform/p2p/socket_dispatcher.cc

Comment 15 by hta@chromium.org on Tue, Feb 16, 2021, 4:34 AM EST Project Member

Status: Fixed (was: Assigned)

Speculatively marking as fixed - original reporter, can you verify?

It should now be impossible to get an UaF according to the previous report, but we might get the P2PSocketManager released on a different thread than previously - I'm not sure if that matters.

Comment 16 by emily...@gmail.com on Tue, Feb 16, 2021, 6:11 AM EST

I tested more than 10+ times with above patch in Chromium 90.0.4408.0. And never repro crash again.

Comment 17 by sheriffbot on Tue, Feb 16, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Tue, Feb 16, 2021, 1:57 PM EST Project Member

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

Comment 19 by sheriffbot on Tue, Feb 16, 2021, 2:17 PM EST Project Member

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

Requesting merge to stable M88 because latest trunk commit (854050) appears to be after stable branch point (827102).

Requesting merge to beta M89 because latest trunk commit (854050) appears to be after beta branch point (843830).

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

Comment 20 by sheriffbot on Tue, Feb 16, 2021, 2:19 PM EST Project Member

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

This bug requires manual review: We are only 13 days from stable.
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 21 by gov...@chromium.org on Tue, Feb 16, 2021, 3:00 PM EST Project Member

Cc: adetaylor@chromium.org amyressler@google.com benmason@chromium.org pbomm...@chromium.org

+Security TPMs for merge review.

Comment 22 by adetaylor@chromium.org on Wed, Feb 17, 2021, 11:20 AM EST Project Member

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

Approving merge to M89, branch 4389, BUT please could you wait for 72 hours' Canary coverage before merging. (Just because any change which alters object lifecycle threading could have unforeseen implications).

Comment 23 by hta@chromium.org on Thu, Feb 18, 2021, 3:49 AM EST Project Member

NextAction: 2021-02-19

Adding NextAction on Friday, Feb 19 (Branch tag for 90.0.4420 was Feb 16, if I read it correctly).

Comment 24 by hta@chromium.org on Mon, Feb 22, 2021, 7:54 AM EST Project Member

Responding to #20:
1. Yes, fix is a pri 1 security bug with low complexity fix
2. https://chromium-review.googlesource.com/c/chromium/src/+/2692532
3. Yes.
4. Sheriffbot requested merge to 89 and 88. Merge to 89 is in progress (https://chromium-review.googlesource.com/c/chromium/src/+/2709590)
5. Pri 1 security bug (I note that it doesn't seem to have happened in the field, so merge to stable may not be needed)
6. No.
7. N/A

Summary: My personal evaluation is that this is unlikely to be problematic if left unpatched in 88. But the fix is low complexity, so if we're spinning a new 88 anyway, we might as well include it.

Comment 25 by bugdroid on Mon, Feb 22, 2021, 8:17 AM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6ed1c0c425e03172c77ba0f1465fe3ade79f2b2a

commit 6ed1c0c425e03172c77ba0f1465fe3ade79f2b2a
Author: Harald Alvestrand <hta@chromium.org>
Date: Mon Feb 22 13:13:58 2021

[Merge to M89] Fix GetP2PSocketManager ownership

Let it return a mojo::SharedRemote<> instead of a raw pointer - this is
a decoration around a shared_refptr.

(cherry picked from commit 82cdc0781ceb4c22ef5903cf3115bea518a5523b)

~~Bug: chromium:1172054~~
Change-Id: I49bd22a0dc949bf869744d2ad25c1afcaea7fdbc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2692532
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#854050}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2709590
Reviewed-by: Harald Alvestrand <hta@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#1280}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/6ed1c0c425e03172c77ba0f1465fe3ade79f2b2a/third_party/blink/renderer/platform/p2p/socket_dispatcher.h
[modify] https://crrev.com/6ed1c0c425e03172c77ba0f1465fe3ade79f2b2a/third_party/blink/renderer/platform/p2p/socket_dispatcher.cc

Comment 26 by adetaylor@chromium.org on Mon, Feb 22, 2021, 10:48 AM EST Project Member

There's very unlikely to be another security-relevant M88 release anyway, but I'll keep the merge-request label there just in case. Thanks for the answers.

Re:
> (I note that it doesn't seem to have happened in the field, so merge to stable may not be needed)

JFYI we tend not to use that as a decision criterion, because attackers exploiting this won't show up in our crash reporting systems (unless they mess up!) Their goal is to use the same bug to craft heap corruption without crashing but instead to achieve remote code execution.

Comment 27 by adetaylor@google.com on Mon, Feb 22, 2021, 3:01 PM EST Project Member

Labels: -Restrict-View-SecurityNotify Restrict-View-SecurityNotifyWebRTC

Testing out whether we can make this bug visible to the WebRTC security notify community as well as our standard security notify community.

Comment 28 by amyressler@google.com on Wed, Feb 24, 2021, 6:40 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 29 by amyressler@google.com on Wed, Feb 24, 2021, 7:21 PM EST Project Member

Congratulations! The VRP Panel has decide to award you $5,000 for this report. Nice work!

Comment 30 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 31 by amyressler@google.com on Fri, Feb 26, 2021, 3:17 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 32 by adetaylor@google.com on Fri, Feb 26, 2021, 4:44 PM EST Project Member

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

Not merging to M88 - no further releases planned.

Comment 33 by asumaneev@google.com on Mon, Mar 1, 2021, 2:42 PM EST Project Member

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

Comment 34 by adetaylor@google.com on Mon, Mar 1, 2021, 7:26 PM EST Project Member

Labels: CVE-2021-21162 CVE_description-missing

Comment 35 by gianluca@google.com on Tue, Mar 2, 2021, 9:04 AM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 36 by asumaneev@google.com on Tue, Mar 2, 2021, 9:07 AM EST Project Member

Labels: -LTS-Merge-Request-86

Comment 37 by hta@chromium.org on Tue, Mar 2, 2021, 9:47 AM EST Project Member

Now we have 86 patched, 87 and 88 not patched, and 89 patched. I don't know who uses 86, but won't this get them into trouble if they try to upgrade to 87 or 88?

Comment 38 by adetaylor@chromium.org on Tue, Mar 2, 2021, 11:51 AM EST Project Member

That weird situation is in fact intentional. M89 is released today. M86 is supported for ChromeOS only as a long-term support release. So all users should either be on M86 (ChromeOS LTS) or M89 (everyone else).

That's assuming the release of M89 goes as planned...

Comment 39 by bugdroid on Tue, Mar 2, 2021, 12:34 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a4faa754a9ef3f63d0c2d5f2a34859029b748833

commit a4faa754a9ef3f63d0c2d5f2a34859029b748833
Author: Harald Alvestrand <hta@chromium.org>
Date: Tue Mar 02 17:33:49 2021

[Merge to M86-LTS] Fix GetP2PSocketManager ownership

Let it return a mojo::SharedRemote<> instead of a raw pointer - this is
a decoration around a shared_refptr.

(cherry picked from commit 82cdc0781ceb4c22ef5903cf3115bea518a5523b)

(cherry picked from commit 6ed1c0c425e03172c77ba0f1465fe3ade79f2b2a)

~~Bug: chromium:1172054~~
Change-Id: I49bd22a0dc949bf869744d2ad25c1afcaea7fdbc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2692532
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#854050}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2709590
Reviewed-by: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4389@{#1280}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2726713
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Commit-Queue: Artem Sumaneev <asumaneev@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1555}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/a4faa754a9ef3f63d0c2d5f2a34859029b748833/third_party/blink/renderer/platform/p2p/socket_dispatcher.h
[modify] https://crrev.com/a4faa754a9ef3f63d0c2d5f2a34859029b748833/third_party/blink/renderer/platform/p2p/socket_dispatcher.cc

Comment 40 by asumaneev@google.com on Tue, Mar 2, 2021, 12:35 PM EST Project Member

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

Comment 41 by adetaylor@google.com on Mon, Mar 8, 2021, 11:58 AM EST Project Member

Cc: natashenka@google.com

Comment 42 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 43 by sheriffbot on Tue, May 25, 2021, 1:52 PM EDT Project Member

Labels: -Restrict-View-SecurityNotifyWebRTC 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 44 by amyressler@chromium.org on Wed, Jan 5, 2022, 4:43 PM EST Project Member

Hello OP/emilykim@, we consider attachments/pocs included with reports to be an integral part of the report (https://bughunters.google.com/about/rules/5745167867576320), so I've undeleted them. Thank you!