☆ Starred by 1 user

Owner:	mek@chromium.org
CC:	asully@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Storage
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
Arch-x86_64
Deadline-Exceeded
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
reward-6000
Via-Wizard-Security
CVE_description-submitted
Target-97
external_security_report
Target-98
Target-100
FoundIn-97
Security_Impact-Extended
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-2-M100
CVE-2022-1305

Issue 1285234: AddressSanitizer: heap-use-after-free in blink::BlobBytesProvider::AppendData

Reported by m.coo...@gmail.com on Fri, Jan 7, 2022, 5:06 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4676.0 Safari/537.36

Steps to reproduce the problem:
This is found by my fuzzer running on ClusterFuzz, but it cannot be reproduced stably so ClusterFuzz does not automatically open a case.
https://clusterfuzz.com/testcase-detail/4673278891065344 (may require the security team to set permissions)

What is the expected behavior?

What went wrong?
Type of crash
render process

Did this work before? N/A

Chrome version: 100.0.4676.0 Channel: n/a
OS Version: 10.0

#Analysis
CreateAndBind creates a BlobBytesProvider object[1] and binds the life cycle of the BlobBytesProvider object to receiver[2] by MakeSelfOwnedReceiver.
An error in receiver(OnPipeConnectionError) will cause the BlobBytesProvider object to be freed and cause UAF.

```
third_party/blink/renderer/platform/blob/blob_bytes_provider.cc:122
// static
BlobBytesProvider* BlobBytesProvider::CreateAndBind(
    mojo::PendingReceiver<mojom::blink::BytesProvider> receiver) {
  auto task_runner = base::ThreadPool::CreateSequencedTaskRunner(
      {base::MayBlock(), base::TaskPriority::USER_VISIBLE});
  auto provider = base::WrapUnique(new BlobBytesProvider(task_runner)); <<--[1]--
  auto* result = provider.get();
  // TODO(mek): Consider binding BytesProvider on the IPC thread instead, only
  // using the MayBlock taskrunner for actual file operations.
  PostCrossThreadTask(
      *task_runner, FROM_HERE,
      CrossThreadBindOnce(
          [](std::unique_ptr<BlobBytesProvider> provider,
             mojo::PendingReceiver<mojom::blink::BytesProvider> receiver) {
            mojo::MakeSelfOwnedReceiver(std::move(provider),        <<--[2]--
                                        std::move(receiver));
          },

          std::move(provider), std::move(receiver)));
  return result;
}
```

}
```

#Patch
Not yet

#asan

```
===
==359458==ERROR: AddressSanitizer: heap-use-after-free on address 0x604000263e6c at pc 0x55b04d2d7d13 bp
0x7ffd04c242a0 sp 0x7ffd04c24298
READ of size 4 at 0x604000263e6c thread T0 (chrome)
SCARINESS: 45 (4-byte-read-heap-use-after-free)
    #0 0x55b04d2d7d12 in blink::BlobBytesProvider::AppendData(base::span<char const, 18446744073709551615ul>)
third_party/blink/renderer/platform/wtf/vector.h:1184:36
    #1 0x55b04d2e08e7 in blink::BlobData::AppendDataInternal(base::span<char const, 18446744073709551615ul>,
scoped_refptr<blink::RawData>) third_party/blink/renderer/platform/blob/blob_data.cc:305:27
    #2 0x55b04d2e2878 in blink::BlobData::AppendText(WTF::String const&, bool)
third_party/blink/renderer/platform/blob/blob_data.cc
    #3 0x55b05ca600e4 in blink::Blob::PopulateBlobData(blink::BlobData*,
blink::HeapVector<cppgc::internal::BasicMember<blink::V8UnionArrayBufferOrArrayBufferViewOrBlobOrUSVString,
cppgc::internal::StrongMemberTag, cppgc::internal::DijkstraWriteBarrierPolicy, cppgc::internal::DisabledCheckingPolicy>,
0u> const&, bool) third_party/blink/renderer/core/fileapi/blob.cc:174:20
    #4 0x55b05ca5fb57 in blink::Blob::Create(blink::ExecutionContext*,
blink::HeapVector<cppgc::internal::BasicMember<blink::V8UnionArrayBufferOrArrayBufferViewOrBlobOrUSVString,
cppgc::internal::StrongMemberTag, cppgc::internal::DijkstraWriteBarrierPolicy, cppgc::internal::DisabledCheckingPolicy>,
0u> const&, blink::BlobPropertyBag const*) third_party/blink/renderer/core/fileapi/blob.cc:129:3
    #5 0x55b05fce657a in blink::(anonymous
namespace)::v8_blob::ConstructorCallback(v8::FunctionCallbackInfo<v8::Value> const&)
gen/third_party/blink/renderer/bindings/core/v8/v8_blob.cc:155:9
    #6 0x55b04a581e47 in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) v8/src/api/api-
arguments-inl.h:152:3
    #7 0x55b04a57ebed 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:112:36
    #8 0x55b04a57d43e in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*)
v8/src/builtins/builtins-api.cc:138:5
    #9 0x7ec707f08d37 (<unknown module>)
    #10 0x7ec707e89bee (<unknown module>)
    #11 0x7ec707fa9c35 (<unknown module>)
    #12 0x7ec707e8c6a1 (<unknown module>)
    #13 0x7ec707e8c6a1 (<unknown module>)
    #14 0x7ec707e8a6db (<unknown module>)
    #15 0x7ec707e8a406 (<unknown module>)
    #16 0x55b04a86f8d4 in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous
namespace)::InvokeParams const&) v8/src/execution/simulator.h:156:12
    #17 0x55b04a86d563 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:517:10
    #18 0x55b04a49883a in v8::Function::Call(v8::Local<v8::Context>, v8::Local<v8::Value>, int, v8::Local<v8::Value>*)
v8/src/api/api.cc:5304:7

    #19 0x55b05cab9b26 in blink::V8ScriptRunner::CallFunction(v8::Local<v8::Function>, blink::ExecutionContext*,
v8::Local<v8::Value>, int, v8::Local<v8::Value>*, v8::Isolate*)
third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:776:17
```
```

```
third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:776:17
   #20 0x55b05fc0d9ea in blink::bindings::CallbackInvokeHelper<blink::CallbackFunctionBase,
(blink::bindings::CallbackInvokeHelperMode)0>::Call(int, v8::Local<v8::Value>*)
third_party/blink/renderer/bindings/core/v8/callback_invoke_helper.cc:132:10
   #21 0x55b05fc1a789 in blink::V8Function::Invoke(blink::bindings::V8ValueOrScriptWrappableAdapter,
blink::HeapVector<blink::ScriptValue, 0u> const&) gen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:68:15
   #22 0x55b05fc1af5c in blink::V8Function::InvokeAndReportException(blink::bindings::V8ValueOrScriptWrappableAdapter,
blink::HeapVector<blink::ScriptValue, 0u> const&) gen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:135:17
   #23 0x55b05d3124a3 in blink::ScheduledAction::Execute(blink::ExecutionContext*)
third_party/blink/renderer/bindings/core/v8/scheduled_action.cc:135:18
   #24 0x55b05d31044b in blink::DOMTimer::Fired() third_party/blink/renderer/core/frame/dom_timer.cc:210:11
   #25 0x55b05f837389 in blink::TimerBase::RunInternal() third_party/blink/renderer/platform/timer.cc:147:3
   #26 0x55b04fff2552 in base::DefaultDelayedTaskHandleDelegate::RunTask(base::OnceCallback<void ()>)
base/callback.h:142:12
   #27 0x55b04fff27cf in base::internal::Invoker<base::internal::BindState<void
(base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, void
()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:535:12
   #28 0x55b04ffa4183 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/callback.h:142:12
   #29 0x55b04ffe3c43 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) base/task/common/task_annotator.h:74:5
   #30 0x55b04ffe3457 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
   #31 0x55b04ffe4811 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
   #32 0x55b04fe9b45f in base::MessagePumpDefault::Run(base::MessagePump::Delegate*)
base/message_loop/message_pump_default.cc:38:55
   #33 0x55b04ffe4ed7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
   #34 0x55b04ff1e6a9 in base::RunLoop::Run(base::Location const&) base/run_loop.cc:140:14
   #35 0x55b06409b98c in content::RendererMain(content::MainFunctionParams) content/renderer/renderer_main.cc:283:16
   #36 0x55b04ed67640 in content::RunZygote(content::ContentMainDelegate*)
content/app/content_main_runner_impl.cc:615:14
   #37 0x55b04ed6a19e in content::RunOtherNamedProcessTypeMain(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:687:12
   #38 0x55b04ed6c027 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1028:10
   #39 0x55b04ed64b6c in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content/app/content_main.cc:398:36
   #40 0x55b04ed66794 in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:426:10
   #41 0x55b041c7d7fe in ChromeMain chrome/app/chrome_main.cc:177:12
   #42 0x7f2e634e382f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
0x604000263e6c is located 28 bytes inside of 48-byte region [0x604000263e50,0x604000263e80)
freed by thread T4 (ThreadPoolForeg) here:
   #0 0x55b041c7b7bd in operator delete(void*) third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:152:3
   #1 0x55b04d2dc149 in mojo::internal::SelfOwnedReceiver<blink::mojom::blink::BytesProvider>::Close()
buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
   #2 0x55b04d2dbd43 in mojo::internal::SelfOwnedReceiver<blink::mojom::blink::BytesProvider>::OnDisconnect(unsigned
int, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&)

mojo/public/cpp/bindings/self_owned_receiver.h:109:5
   #3 0x55b050adc5f0 in mojo::InterfaceEndpointClient::NotifyError(absl::optional<mojo::DisconnectReason> const&)
base/callback.h:142:12
```

```
base/callback.h:142:12
   #4 0x55b050af8367 in mojo::internal::MultiplexRouter::ProcessNotifyErrorTask(mojo::internal::MultiplexRouter::Task*,
mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*)
mojo/public/cpp/bindings/lib/multiplex_router.cc:1024:13
   #5 0x55b050af1ebe in mojo::internal::MultiplexRouter::ProcessTasks(mojo::internal::MultiplexRouter::ClientCallBehavior,
base::SequencedTaskRunner*) mojo/public/cpp/bindings/lib/multiplex_router.cc:937:15
   #6 0x55b050aee323 in mojo::internal::MultiplexRouter::OnPipeConnectionError(bool)
mojo/public/cpp/bindings/lib/multiplex_router.cc:847:3
   #7 0x55b050acf518 in mojo::Connector::HandleError(bool, bool) base/callback.h:142:12
   #8 0x55b050b40b57 in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&)
base/callback.h:241:12
   #9 0x55b050b41b2f 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:535:12
   #10 0x55b04ffa4183 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/callback.h:142:12
   #11 0x55b05000d02a in base::internal::TaskTracker::RunTaskImpl(base::internal::Task&, base::TaskTraits const&,
base::internal::TaskSource*, base::SequenceToken const&) base/task/common/task_annotator.h:74:5
   #12 0x55b05000df16 in base::internal::TaskTracker::RunSkipOnShutdown(base::internal::Task&, base::TaskTraits const&,
base::internal::TaskSource*, base::SequenceToken const&) base/task/thread_pool/task_tracker.cc:691:3
   #13 0x55b05000c762 in base::internal::TaskTracker::RunTask(base::internal::Task, base::internal::TaskSource*,
base::TaskTraits const&) base/task/thread_pool/task_tracker.cc:721:7
   #14 0x55b0500bf41c in base::internal::TaskTrackerPosix::RunTask(base::internal::Task, base::internal::TaskSource*,
base::TaskTraits const&) base/task/thread_pool/task_tracker_posix.cc:22:16
   #15 0x55b05000bc76 in base::internal::TaskTracker::RunAndPopNextTask(base::internal::RegisteredTaskSource)
base/task/thread_pool/task_tracker.cc:466:5
   #16 0x55b05002437e in base::internal::WorkerThread::RunWorker() base/task/thread_pool/worker_thread.cc:379:34
   #17 0x55b050023731 in base::internal::WorkerThread::RunPooledWorker()
base/task/thread_pool/worker_thread.cc:266:3
   #18 0x55b0500c08b5 in base::(anonymous namespace)::ThreadFunc(void*)
base/threading/platform_thread_posix.cc:98:13
   #19 0x7f2e69f6f6b9 in start_thread /build/glibc-LK5gWL/glibc-2.23/nptl/pthread_create.c:333
previously allocated by thread T0 (chrome) here:
   #0 0x55b041c7af5d in operator new(unsigned long) third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:95:3
   #1 0x55b04d2d671f in
blink::BlobBytesProvider::CreateAndBind(mojo::PendingReceiver<blink::mojom::blink::BytesProvider>)
third_party/blink/renderer/platform/blob/blob_bytes_provider.cc:127:36
   #2 0x55b04d2e015d in blink::BlobData::AppendDataInternal(base::span<char const, 18446744073709551615ul>,
scoped_refptr<blink::RawData>) third_party/blink/renderer/platform/blob/blob_data.cc:289:28
   #3 0x55b04d2e2878 in blink::BlobData::AppendText(WTF::String const&, bool)
third_party/blink/renderer/platform/blob/blob_data.cc
   #4 0x55b05ca600e4 in blink::Blob::PopulateBlobData(blink::BlobData*,
blink::HeapVector<cppgc::internal::BasicMember<blink::V8UnionArrayBufferOrArrayBufferViewOrBlobOrUSVString,
cppgc::internal::StrongMemberTag, cppgc::internal::DijkstraWriteBarrierPolicy, cppgc::internal::DisabledCheckingPolicy>,
0u> const&, bool) third_party/blink/renderer/core/fileapi/blob.cc:174:20
   #5 0x55b05ca5fb57 in blink::Blob::Create(blink::ExecutionContext*,
blink::HeapVector<cppgc::internal::BasicMember<blink::V8UnionArrayBufferOrArrayBufferViewOrBlobOrUSVString,
cppgc::internal::StrongMemberTag, cppgc::internal::DijkstraWriteBarrierPolicy, cppgc::internal::DisabledCheckingPolicy>,
0u> const&, blink::BlobPropertyBag const*) third_party/blink/renderer/core/fileapi/blob.cc:129:3
   #6 0x55b05fce657a in blink::(anonymous
namespace)::v8_blob::ConstructorCallback(v8::FunctionCallbackInfo<v8::Value> const&)
gen/third_party/blink/renderer/bindings/core/v8/v8_blob.cc:155:9

   #7 0x55b04a581e47 in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) v8/src/api/api-
arguments-inl.h:152:3
   #8 0x55b04a57ebad in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous
   #8 0x55b04a57ebed 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:112:36
   #9 0x55b04a57d43e in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*)
v8/src/builtins/builtins-api.cc:138:5
   #10 0x7ec707f08d37  (<unknown module>)
   #11 0x7ec707e89bee  (<unknown module>)
   #12 0x7ec707fa9c35  (<unknown module>)
   #13 0x7ec707e8c6a1  (<unknown module>)
   #14 0x7ec707e8c6a1  (<unknown module>)
   #15 0x7ec707e8a6db  (<unknown module>)
   #16 0x7ec707e8a406  (<unknown module>)
   #17 0x55b04a86f8d4 in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous
namespace)::InvokeParams const&) v8/src/execution/simulator.h:156:12
   #18 0x55b04a86d563 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:517:10
   #19 0x55b04a49883a in v8::Function::Call(v8::Local<v8::Context>, v8::Local<v8::Value>, int, v8::Local<v8::Value>*)
v8/src/api/api.cc:5304:7
   #20 0x55b05cab9b26 in blink::V8ScriptRunner::CallFunction(v8::Local<v8::Function>, blink::ExecutionContext*,
v8::Local<v8::Value>, int, v8::Local<v8::Value>*, v8::Isolate*)
third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:776:17
   #21 0x55b05fc0d9ea in blink::bindings::CallbackInvokeHelper<blink::CallbackFunctionBase,
(blink::bindings::CallbackInvokeHelperMode)0>::Call(int, v8::Local<v8::Value>*)
third_party/blink/renderer/bindings/core/v8/callback_invoke_helper.cc:132:10
   #22 0x55b05fc1a789 in blink::V8Function::Invoke(blink::bindings::V8ValueOrScriptWrappableAdapter,
blink::HeapVector<blink::ScriptValue, 0u> const&) gen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:68:15
   #23 0x55b05fc1af5c in blink::V8Function::InvokeAndReportException(blink::bindings::V8ValueOrScriptWrappableAdapter,
blink::HeapVector<blink::ScriptValue, 0u> const&) gen/third_party/blink/renderer/bindings/core/v8/v8_function.cc:135:17
   #24 0x55b05d3124a3 in blink::ScheduledAction::Execute(blink::ExecutionContext*)
third_party/blink/renderer/bindings/core/v8/scheduled_action.cc:135:18
   #25 0x55b05d31044b in blink::DOMTimer::Fired() third_party/blink/renderer/core/frame/dom_timer.cc:210:11
   #26 0x55b05f837389 in blink::TimerBase::RunInternal() third_party/blink/renderer/platform/timer.cc:147:3
   #27 0x55b04fff2552 in base::DefaultDelayedTaskHandleDelegate::RunTask(base::OnceCallback<void ()>)
base/callback.h:142:12
   #28 0x55b04fff27cf in base::internal::Invoker<base::internal::BindState<void
(base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>),
base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, void
()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:535:12
   #29 0x55b04ffa4183 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/callback.h:142:12
Thread T4 (ThreadPoolForeg) created by T2 (ThreadPoolForeg) here:
   #0 0x55b041c3257c in pthread_create third_party/llvm/compiler-rt/lib/asan/asan_interceptors.cpp:208:3
   #1 0x55b0500bfb5e in base::(anonymous namespace)::CreateThread(unsigned long, bool,
base::PlatformThread::Delegate*, base::PlatformThreadHandle*, base::ThreadPriority)
base/threading/platform_thread_posix.cc:141:13
   #2 0x55b050022a3f in base::internal::WorkerThread::Start(base::WorkerThreadObserver*)
base/task/thread_pool/worker_thread.cc:109:3
   #3 0x55b05001dd55 in void
base::internal::ThreadGroupImpl::ScopedCommandsExecutor::WorkerContainer::ForEachWorker<base::internal::ThreadGro
upImpl::ScopedCommandsExecutor::FlushImpl()::'lambda0'(base::internal::WorkerThread*)>

(base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl()::'lambda0'(base::internal::WorkerThread*))
base/task/thread_pool/thread_group_impl.cc:185:15
   #4 0x55b05001d8bf in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl()
   #4 0x55b05001d8bf in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl()
base/task/thread_pool/thread_group_impl.cc:184:23
   #5 0x55b050017656 in
base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushWorkerCreation(base::internal::CheckedLock*)
base/task/thread_pool/thread_group_impl.cc:117:5
   #6 0x55b050016dc9 in
base::internal::ThreadGroupImpl::WorkerThreadDelegateImpl::GetWork(base::internal::WorkerThread*)
base/task/thread_pool/thread_group_impl.cc:617:14
   #7 0x55b0500242de in base::internal::WorkerThread::RunWorker() base/task/thread_pool/worker_thread.cc:360:51
   #8 0x55b050023731 in base::internal::WorkerThread::RunPooledWorker() base/task/thread_pool/worker_thread.cc:266:3
   #9 0x55b0500c08b5 in base::(anonymous namespace)::ThreadFunc(void*)
base/threading/platform_thread_posix.cc:98:13
   #10 0x7f2e69f6f6b9 in start_thread /build/glibc-LK5gWL/glibc-2.23/nptl/pthread_create.c:333
Thread T2 (ThreadPoolForeg) created by T0 (chrome) here:
   #0 0x55b041c3257c in pthread_create third_party/llvm/compiler-rt/lib/asan/asan_interceptors.cpp:208:3
   #1 0x55b0500bfb5e in base::(anonymous namespace)::CreateThread(unsigned long, bool,
base::PlatformThread::Delegate*, base::PlatformThreadHandle*, base::ThreadPriority)
base/threading/platform_thread_posix.cc:141:13
   #2 0x55b050022a3f in base::internal::WorkerThread::Start(base::WorkerThreadObserver*)
base/task/thread_pool/worker_thread.cc:109:3
   #3 0x55b05001dd55 in void
base::internal::ThreadGroupImpl::ScopedCommandsExecutor::WorkerContainer::ForEachWorker<base::internal::ThreadGro
upImpl::ScopedCommandsExecutor::FlushImpl()::'lambda0'(base::internal::WorkerThread*)>
(base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl()::'lambda0'(base::internal::WorkerThread*))
base/task/thread_pool/thread_group_impl.cc:185:15
   #4 0x55b05001d8bf in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::FlushImpl()
base/task/thread_pool/thread_group_impl.cc:184:23
   #5 0x55b050014d08 in base::internal::ThreadGroupImpl::ScopedCommandsExecutor::~ScopedCommandsExecutor()
base/task/thread_pool/thread_group_impl.cc:103:31
   #6 0x55b05001427b in base::internal::ThreadGroupImpl::Start(int, int, base::TimeDelta,
scoped_refptr<base::SequencedTaskRunner>, base::WorkerThreadObserver*,
base::internal::ThreadGroup::WorkerEnvironment, bool, absl::optional<base::TimeDelta>)
base/task/thread_pool/thread_group_impl.cc:440:1
   #7 0x55b04fff74bb in base::internal::ThreadPoolImpl::Start(base::ThreadPoolInstance::InitParams const&,
base::WorkerThreadObserver*) base/task/thread_pool/thread_pool_impl.cc:230:11
   #8 0x55b05be6756a in content::ChildProcess::ChildProcess(base::ThreadPriority, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, std::__1::unique_ptr<base::ThreadPoolInstance::InitParams,
std::__1::default_delete<base::ThreadPoolInstance::InitParams> >) content/child/child_process.cc:80:40
   #9 0x55b06200f6a2 in content::RenderProcess::RenderProcess(std::__1::basic_string<char, std::__1::char_traits<char>,
std::__1::allocator<char> > const&, std::__1::unique_ptr<base::ThreadPoolInstance::InitParams,
std::__1::default_delete<base::ThreadPoolInstance::InitParams> >) content/renderer/render_process.cc:28:7
   #10 0x55b06200eeb4 in content::RenderProcessImpl::RenderProcessImpl()
content/renderer/render_process_impl.cc:100:7
   #11 0x55b06200f5ea in content::RenderProcessImpl::Create() content/renderer/render_process_impl.cc:297:31
   #12 0x55b06409b515 in content::RendererMain(content::MainFunctionParams)
content/renderer/renderer_main.cc:226:53
   #13 0x55b04ed67640 in content::RunZygote(content::ContentMainDelegate*)
content/app/content_main_runner_impl.cc:615:14
   #14 0x55b04ed6a19e in content::RunOtherNamedProcessTypeMain(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:687:12

   #15 0x55b04ed6c027 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1028:10
   #16 0x55b04ed64b6c in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
content/app/content_main.cc:398:36
```

```
content/app/content_main.cc:398:36
    #17 0x55b04ed66794 in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:426:10
    #18 0x55b041c7d7fe in ChromeMain chrome/app/chrome_main.cc:177:12
    #19 0x7f2e634e382f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
SUMMARY: AddressSanitizer: heap-use-after-free third_party/blink/renderer/platform/wtf/vector.h:1184:36 in
blink::BlobBytesProvider::AppendData(base::span<char const, 18446744073709551615ul>)
Shadow bytes around the buggy address:
  0x0c0880044770: fa fa 00 00 00 00 00 fa fa fa 00 00 00 00 00 fa
  0x0c0880044780: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 00
  0x0c0880044790: fa fa 00 00 00 00 00 00 fa fa 00 00 00 00 00 fa
  0x0c08800447a0: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
  0x0c08800447b0: fa fa fd fd fd fd fd fa fa fa 00 00 00 00 00 fa
=>0x0c08800447c0: fa fa fd fd fd fd fd fa fa fa fd fd fd[fd]fd fd
  0x0c08800447d0: fa fa 00 00 00 00 00 fa fa fa fa fa fa fa fa fa
  0x0c08800447e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c08800447f0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0880044800: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c0880044810: 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
==359458==ABORTING
```

Comment 1 by sheriffbot on Fri, Jan 7, 2022, 5:08 AM EST

Labels: external_security_report

Comment 2 by drubery@chromium.org on Fri, Jan 7, 2022, 12:39 PM EST

Status: Assigned (was: Unconfirmed)
Owner: dmu...@chromium.org
Labels: Security_Severity-High FoundIn-97
Components: Blink>Storage

This sounds reasonable, and ClusterFuzz can sometimes reproduce it. Adding security labels and triaging to a code owner. The affected code is in M97, so marking FoundIn-97, even though ClusterFuzz couldn't bisect it.

Comment 3 by sheriffbot on Fri, Jan 7, 2022, 12:39 PM EST

Labels: Security_Impact-Stable

Comment 4 by sheriffbot on Fri, Jan 7, 2022, 12:47 PM EST

Labels: Target-97 M-97

Setting milestone and target because of high severity.

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

Comment 5 by sheriffbot on Fri, Jan 7, 2022, 1:07 PM EST

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 dmu...@chromium.org on Tue, Jan 11, 2022, 4:09 PM EST

Owner: mek@chromium.org

-> Storage TL

Comment 7 by sheriffbot on Fri, Jan 21, 2022, 12:21 PM EST

mek: 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 8 by mek@chromium.org on Fri, Jan 21, 2022, 12:38 PM EST

security team: can you set the permissions for the clusterfuzz report/link it to this issue so that I can access it (as requested in the original report)?

"An error in receiver(OnPipeConnectionError) will cause the BlobBytesProvider object to be freed and cause UAF." is certainly true. Although I am surprised that it is possible to get such an error... BlobBytesProvider is only accessed while we still own the remote end of the mojo pipe (and nothing is send over that remote). So not sure what would be triggering such a connection error. Hopefully the repro case sheds some light on what is going on...

Comment 9 by m.coo...@gmail.com on Fri, Jan 21, 2022, 8:40 PM EST

upload testcase form clusterfuzz.
Note that they are not stable to reproduce.

[Deleted] **2022-01-22 093909.png**

clusterfuzz-testcase-4673278891065344.zip
127 KB Download

clusterfuzz-testcase-5340199057686528.zip
68.0 KB Download

Comment 10 by m.coo...@gmail.com on Fri, Jan 21, 2022, 8:41 PM EST

Reproduction parameters for #c09

1. https://clusterfuzz.com/testcase-detail/5340199057686528
Crash State:
blink::BlobBytesProvider::AppendData
blink::BlobData::AppendDataInternal
blink::MediaRecorder::WriteData
Crash Type: Heap-use-after-free READ 4

ORIGINAL STACKTRACE ON REVISION 956865 (1431 LINES)

```
[Environment]
ASAN_OPTIONS=alloc_dealloc_mismatch=0:allocator_may_return_null=0:allow_user_segv_handler=0:check_malloc_usable_size=0:detect_leaks=0:detect_odr_violation=0:detect_stack_use_after_return=1:fast_unwind_on_fatal=1:handle_abort=1:handle_segv=1:handle_sigbus=1:handle_sigfpe=1:handle_sigill=1:max_uar_stack_size_log=16:print_scariness=1:print_summary=1:print_suppressions=0:redzone=32:strict_memcmp=0:symbolize=0:use_sigaltstack=1
[Command line] /mnt/scratch0/clusterfuzz/bot/builds/chromium-browser-asan_linux-release_4392242b7f59878a2775b4607420a2b37e17ff13/revisions/asan-linux-release-956865/chrome --user-data-dir=/mnt/scratch0/tmp/user_profile_0 --ignore-gpu-blacklist --allow-file-access-from-files --disable-gesture-requirement-for-media-playback --disable-click-to-play --disable-hang-monitor --dns-prefetch-disable --disable-default-apps --disable-component-update --safebrowsing-disable-auto-update --metrics-recording-only --disable-gpu-watchdog --disable-metrics --disable-popup-blocking --disable-prompt-on-repost --enable-experimental-extension-apis --enable-extension-apps --js-flags="--expose-gc --verify-heap" --new-window --no-default-browser-check --no-first-run --no-process-singleton-dialog --enable-shadow-dom --enable-media-stream --use-gl=angle --use-angle=swiftshader --use-cmd-decoder=passthrough --use-fake-device-for-media-stream --use-fake-ui-for-media-stream --disable-in-process-stack-traces --enable-logging=stderr --v=1 --disable-field-trial-config --enable-benchmarking /mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases/fuzz-00636.html
```

2. https://clusterfuzz.com/testcase-detail/4673278891065344

Crash State:
blink::BlobBytesProvider::AppendData
blink::BlobData::AppendDataInternal
blink::BlobData::AppendText
Crash Type: Heap-use-after-free READ 4

ORIGINAL STACKTRACE ON REVISION 956357 (1418 LINES)

```
[Environment]
ASAN_OPTIONS=alloc_dealloc_mismatch=0:allocator_may_return_null=1:allow_user_segv_handler=0:check_malloc_usable_size=0:detect_leaks=1:detect_odr_violation=0:detect_stack_use_after_return=1:external_symbolizer_path=/mnt/scratch0/clusterfuzz/resources/platform/linux/llvm-symbolizer:fast_unwind_on_fatal=1:handle_abort=1:handle_segv=1:handle_sigbus=1:handle_sigfpe=1:handle_sigill=1:max_uar_stack_size_log=16:print_scariness=1:print_summary=1:print_suppressions=0:redzone=16:strict_memcmp=0:symbolize=1:symbolize_inline_frames=false:use_sigaltstack=1
[Command line] /mnt/scratch0/clusterfuzz/bot/builds/chromium-browser-asan_linux-release_4392242b7f59878a2775b4607420a2b37e17ff13/revisions/asan-linux-release-956357/chrome --user-data-dir=/mnt/scratch0/tmp/user_profile_0 --ignore-gpu-blacklist --allow-file-access-from-files --disable-gesture-requirement-for-media-playback --disable-click-to-play --disable-hang-monitor --dns-prefetch-disable --disable-default-apps --disable-component-update --safebrowsing-disable-auto-update --metrics-recording-only --disable-gpu-watchdog --disable-metrics --disable-popup-blocking --disable-prompt-on-repost --enable-experimental-extension-apis --enable-extension-apps --js-
```

```
disable-popup-blocking --disable-prompt-on-repost --enable-experimental-extension-apis --enable-extension-apps --js-flags="--expose-gc --verify-heap" --new-window --no-default-browser-check --no-first-run --no-process-singleton-dialog --enable-shadow-dom --enable-media-stream --use-gl=angle --use-angle=swiftshader --use-fake-device-for-media-stream --use-fake-ui-for-media-stream --no-sandbox --disable-in-process-stack-traces --enable-logging=stderr --v=1 --enable-experimental-web-platform-features /mnt/scratch0/clusterfuzz/bot/inputs/fuzzer-testcases/fuzz-00255.html
```

Comment 11 by sheriffbot on Tue, Feb 1, 2022, 5:37 PM EST

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 12 by sheriffbot on Wed, Feb 2, 2022, 12:21 PM EST

Labels: -M-97 M-98 Target-98

Comment 13 by sheriffbot on Sat, Feb 5, 2022, 12:21 PM EST

mek: 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 14 by m.coo...@gmail.com on Thu, Feb 24, 2022, 9:50 AM EST

ping @mek

Comment 15 by sheriffbot on Tue, Mar 8, 2022, 1:46 PM EST

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 16 Deleted

Comment 17 by adetaylor@google.com on Thu, Mar 24, 2022, 7:58 PM EDT

Cc: asully@chromium.org

Comment 18 by adetaylor@google.com on Fri, Mar 25, 2022, 4:04 PM EDT

mek@ has a speculative fix out for review: https://chromium-review.googlesource.com/c/chromium/src/+/3553304

Comment 19 by Git Watcher on Mon, Mar 28, 2022, 4:13 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7222e9825fc02acc962e005c59885ee2f26df185

commit 7222e9825fc02acc962e005c59885ee2f26df185
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Mon Mar 28 20:12:14 2022

Change ownership of BlobBytesProvider.

Rather than immediately passing ownership to a cross-thread
SelfOwnedReceiver while retaining a raw pointer, instead maintain
ownership in a unique_ptr as long as it is needed, only transferring
ownership to a SelfOwnedReceiver when BlobData is done with the
BlobBytesProvider.

Also clean-up/tighten down sequence checks for BlobBytesProvider a bit.

~~Bug: 1285234~~
Change-Id: I7273e886a0bab2ae489b680d786991c9e4ff1dbb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3553304
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Commit-Position: refs/heads/main@{#986111}

[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_data.h
[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_bytes_provider.h
[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_bytes_provider_test.cc
[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_bytes_provider.cc
[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_data.cc
[modify]
https://crrev.com/7222e9825fc02acc962e005c59885ee2f26df185/third_party/blink/renderer/platform/blob/blob_data_test.cc

Comment 20 by mek@chromium.org on Tue, Mar 29, 2022, 12:58 AM EDT

Status: Fixed (was: Assigned)

Comment 21 by sheriffbot on Tue, Mar 29, 2022, 12:41 PM EDT

Labels: reward-topanel

Comment 22 by sheriffbot on Tue, Mar 29, 2022, 1:40 PM EDT

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

Comment 23 by sheriffbot on Tue, Mar 29, 2022, 2:01 PM EDT

Labels: Merge-Request-101 Merge-Request-100 Merge-Request-98 Merge-Request-99

Requesting merge to extended stable M98 because latest trunk commit (986111) appears to be after extended stable

Requesting merge to extended stable M98 because latest trunk commit (986111) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (986111) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (986111) appears to be after beta branch point (972766).

Requesting merge to dev M101 because latest trunk commit (986111) appears to be after dev branch point (982481).

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

Comment 24 by sheriffbot on Tue, Mar 29, 2022, 4:17 PM EDT

Labels: -Merge-Request-101 Hotlist-Merge-Approved Merge-Approved-101

Merge approved: your change passed merge requirements and is auto-approved for M101. Please go ahead and merge the CL to branch 4951 (refs/branch-heads/4951) 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: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 25 by sheriffbot on Tue, Mar 29, 2022, 4:17 PM EDT

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 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 26 by sheriffbot on Tue, Mar 29, 2022, 4:17 PM EDT

Labels: -Merge-Request-99 Merge-Review-99

Merge review required: M99 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?

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 27 by Git Watcher on Tue, Mar 29, 2022, 7:13 PM EDT

Labels: -merge-approved-101 merge-merged-4951 merge-merged-101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7187b41cd6201840c8c66f6ccb88c5907c5f11bc

commit 7187b41cd6201840c8c66f6ccb88c5907c5f11bc
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Tue Mar 29 23:12:33 2022

M101: Change ownership of BlobBytesProvider.

Rather than immediately passing ownership to a cross-thread
SelfOwnedReceiver while retaining a raw pointer, instead maintain
ownership in a unique_ptr as long as it is needed, only transferring
ownership to a SelfOwnedReceiver when BlobData is done with the
BlobBytesProvider.

Also clean-up/tighten down sequence checks for BlobBytesProvider a bit.

(cherry picked from commit 7222e9825fc02acc962e005c59885ee2f26df185)

~~Bug: 1285234~~
Change-Id: I7273e886a0bab2ae489b680d786991c9e4ff1dbb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3553304
Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986111}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3557907
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4951@{#246}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_data.h
[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_bytes_provider.h
[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_bytes_provi

https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_bytes_provider_test.cc
[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_bytes_provider.cc
[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_data.cc
[modify]
https://crrev.com/7187b41cd6201840c8c66f6ccb88c5907c5f11bc/third_party/blink/renderer/platform/blob/blob_data_test.cc

Comment 28 by sheriffbot on Wed, Mar 30, 2022, 12:22 PM EDT

Labels: -M-98 M-100 Target-100

Comment 29 by amyressler@chromium.org on Mon, Apr 4, 2022, 5:49 PM EDT

Labels: -Restrict-View-SecurityEmbargo

removing RV-SE based on off-bug comms with researcher

Comment 30 by amyressler@chromium.org on Mon, Apr 4, 2022, 5:52 PM EDT

Labels: -Merge-Request-98 -Merge-Review-99 -Merge-Review-100 Merge-Approved-100

m100 merge approved; please ensure there are no stability issues or other concerns about or exhibited from canary or beta and merge fix to branch 4896 at your earliest convenience

M100 is now Stable channel, merge-na for M99 and M98

Comment 31 by Git Watcher on Tue, Apr 5, 2022, 4:10 PM EDT

Labels: -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f

commit 5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f
Author: Marijn Kruisselbrink <mek@chromium.org>
Date: Tue Apr 05 20:09:23 2022

M100: Change ownership of BlobBytesProvider.

Rather than immediately passing ownership to a cross-thread
SelfOwnedReceiver while retaining a raw pointer, instead maintain
ownership in a unique_ptr as long as it is needed, only transferring
ownership to a SelfOwnedReceiver when BlobData is done with the
BlobBytesProvider.

Also clean-up/tighten down sequence checks for BlobBytesProvider a bit.

(cherry picked from commit 7222e9825fc02acc962e005c59885ee2f26df185)

~~Bug: 1285234~~
Change-Id: I7273e886a0bab2ae489b680d786991c9e4ff1dbb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3553304

Reviewed-by: Austin Sullivan <asully@chromium.org>
Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986111}

Cr-Original-Commit-Position: refs/heads/main@{#986111}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3568972
Auto-Submit: Marijn Kruisselbrink <mek@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4896@{#1040}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_data.h
[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_bytes_provider.h
[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_bytes_provider_test.cc
[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_bytes_provider.cc
[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_data_test.cc
[modify]
https://crrev.com/5cb934a23ddfccb7ce7ace36b5f0ec5036281e0f/third_party/blink/renderer/platform/blob/blob_data.cc

Comment 32 by amyressler@google.com on Mon, Apr 11, 2022, 1:06 PM EDT

Labels: -reward-topanel reward-unpaid reward-6000

*** 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 33 by amyressler@chromium.org on Mon, Apr 11, 2022, 1:13 PM EDT

Congratulations! The VRP Panel has decided to award you $5,000 for this report + a $1,000 fuzzer bonus. Thank you for your efforts and contributions to Chrome Fuzzing as well as still manually reporting this issue to us.

Comment 34 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT

Labels: Release-2-M100

Comment 35 by adetaylor@google.com on Mon, Apr 11, 2022, 1:29 PM EDT

Labels: CVE-2022-1305 CVE_description-missing

Comment 36 by amyressler@google.com on Tue, Apr 12, 2022, 9:19 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 37 by sheriffbot on Tue, Jul 5, 2022, 1:31 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

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

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

Comment 38 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 39 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing

About Monorail　User Guide　Release Notes　Feedback on Monorail　Terms　Privacy