Starred by 2 users

Owner: kron@chromium.org

CC: steveanton@chromium.org
tommi@chromium.org
guidou@chromium.org
hbos@chromium.org
hta@chromium.org
orphis@chromium.org
mbonadei@chromium.org

Status: Fixed *(Closed)*

Components: Blink>WebRTC>Perf

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Windows

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
reward-6000
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-99
Target-99
FoundIn-99
Merge-NA-99
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1133

Issue 1305776: AddressSanitizer: use-after-poison in blink::WebrtcVideoPerfReporter::InitializeOnTaskRunner webrtc_video_perf_reporter.cc:36

Reported by m.coo...@gmail.com on Sat, Mar 12, 2022, 10:35 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.0 Safari/537.36

Steps to reproduce the problem:
#Reproduce
The problem was found by my fuzzer running on CF(CC Security team for access permission
https://clusterfuzz.com/testcase-detail/6544221896769536),
But because it cannot be reproduced stably, CF does not automatically report.
By manual review, it is found that the window time triggered by the vulnerability is very short, so it cannot be reproduced stably.
I will give a detailed vulnerability analysis later.

What is the expected behavior?

What went wrong?
Type of crash
render tab

#Analysis
The issue was introduced by CL(https://chromium-review.googlesource.com/c/chromium/src/+/3472847)

1. PeerConnectionDependencyFactory is on-heap object, and there is a member WebrtcVideoPerfReporter is off-heap object.[3,4]
2. When PeerConnectionDependencyFactory is constructed[2], the WebrtcVideoPerfReporter::Initialize will be called[1], and eventually a new task will be created using WebrtcVideoPerfReporter's weak_this_ as this and post to task_runner_[1].
3. Because PeerConnectionDependencyFactory is an on-heap object, the destructor will not be called immediately when PeerConnectionDependencyFactory is GCed,
so the weak_this_ of WebrtcVideoPerfReporter will not be reset, resulting in UAP.
4. PeerConnectionDependencyFactory uses CleanupPeerConnectionFactory to do some cleanup[5],
so we can invalidate WebrtcVideoPerfReporter's weak_this_ here to fix the problem, I'll provide a patch ASAP.

```
//third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc:21
void WebrtcVideoPerfReporter::Initialize(
    scoped_refptr<base::SingleThreadTaskRunner> task_runner,
    mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>
        perf_recorder) {
  task_runner_ = task_runner;
  task_runner_->PostTask(
      FROM_HERE,
      base::BindOnce(&WebrtcVideoPerfReporter::InitializeOnTaskRunner,
                     weak_this_, std::move(perf_recorder)));                    <<[1]

}

//third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc:405
```

```
//third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc:405
PeerConnectionDependencyFactory::PeerConnectionDependencyFactory(
    : public GarbageCollected<PeerConnectionDependencyFactory>,
      public Supplement<ExecutionContext>,
      public ExecutionContextLifecycleObserver {
  USING_PRE_FINALIZER(PeerConnectionDependencyFactory,                    <<[5]
                      CleanupPeerConnectionFactory);
...CUT...
  webrtc_video_perf_reporter_.Initialize(                                 <<[2]
      context.GetTaskRunner(TaskType::kInternalMedia),
      std::move(perf_recorder));
}

//third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.h:58
class MODULES_EXPORT PeerConnectionDependencyFactory
    : public GarbageCollected<PeerConnectionDependencyFactory>,
      public Supplement<ExecutionContext>,
      public ExecutionContextLifecycleObserver {
  USING_PRE_FINALIZER(PeerConnectionDependencyFactory,
                      CleanupPeerConnectionFactory);

 public:
...CUT...
  WebrtcVideoPerfReporter webrtc_video_perf_reporter_;                    <<[3]

  bool encode_decode_capabilities_reported_ = false;

  THREAD_CHECKER(thread_checker_);
};

class MODULES_EXPORT WebrtcVideoPerfReporter {
 public:
...CUT...

  base::WeakPtr<WebrtcVideoPerfReporter> weak_this_;
  scoped_refptr<base::SingleThreadTaskRunner> task_runner_;
  mojo::Remote<media::mojom::blink::WebrtcVideoPerfRecorder> perf_recorder_;
  base::WeakPtrFactory<WebrtcVideoPerfReporter> weak_factory_{this};      <<[4]
};
```

#Patch
PeerConnectionDependencyFactory uses CleanupPeerConnectionFactory to do some cleanup[5],
so we can invalidate WebrtcVideoPerfReporter's weak_this_ here to fix the problem, I'll provide a patch ASAP.

#asan
```
==================================================================
==1==ERROR: AddressSanitizer: use-after-poison on address 0x7ea500ed43b8 at pc 0x55695ce10735 bp 0x7ffc53a912b0
sp 0x7ffc53a912a8
READ of size 8 at 0x7ea500ed43b8 thread T0 (chrome)
SCARINESS: 33 (8-byte-read-use-after-poison)

    #0 0x55695ce10734 in is_valid mojo/public/cpp/system/handle.h:167:34
    #1 0x55695ce10734 in CloseIfNecessary mojo/public/cpp/system/handle.h:138:17
    #2 0x55695ce10734 in operator= mojo/public/cpp/system/handle.h:93:7
```

#2 0x55695ce10734 in operator= mojo/public/cpp/system/handle.h:93:7
#3 0x55695ce10734 in mojo::internal::InterfacePtrStateBase::Bind(mojo::internal::PendingRemoteState*, scoped_refptr<base::SequencedTaskRunner>) mojo/public/cpp/bindings/lib/interface_ptr_state.cc:64:11
#4 0x55696ddb68c6 in Bind mojo/public/cpp/bindings/lib/interface_ptr_state.h:195:28
#5 0x55696ddb68c6 in Bind mojo/public/cpp/bindings/remote.h:277:21
#6 0x55696ddb68c6 in Bind mojo/public/cpp/bindings/remote.h:262:5
#7 0x55696ddb68c6 in blink::WebrtcVideoPerfReporter::InitializeOnTaskRunner(mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>) third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc:36:18
#8 0x55696ddb756f in void base::internal::FunctorTraits<void (blink::WebrtcVideoPerfReporter::*)(mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>), void>::Invoke<void (blink::WebrtcVideoPerfReporter::*)(mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>), base::WeakPtr<blink::WebrtcVideoPerfReporter>, mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>>(void (blink::WebrtcVideoPerfReporter::*)(mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>), base::WeakPtr<blink::WebrtcVideoPerfReporter>&&, mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>&&) base/bind_internal.h:542:12
#9 0x55695c2d2123 in Run base/callback.h:142:12
#10 0x55695c2d2123 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/task/common/task_annotator.cc:135:32
#11 0x55695c31472d in RunTask<(lambda at ../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:29)> base/task/common/task_annotator.h:74:5
#12 0x55695c31472d in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:385:21
#13 0x55695c313e24 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:290:41
#14 0x55695c315411 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0
#15 0x55695c1c9506 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_default.cc:38:55
#16 0x55695c315ad7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
#17 0x55695c24b129 in base::RunLoop::Run(base::Location const&) base/run_loop.cc:141:14
#18 0x5569709dd93c in content::RendererMain(content::MainFunctionParams) content/renderer/renderer_main.cc:290:16
#19 0x55695b0bbdd8 in content::RunZygote(content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:611:14
#20 0x55695b0bd8d3 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:693:12
#21 0x55695b0bf67f in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1044:10
#22 0x55695b0b91c8 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*) content/app/content_main.cc:407:36
#23 0x55695b0b98ac in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:435:10
#24 0x55694d5b11d6 in ChromeMain chrome/app/chrome_main.cc:176:12
#25 0x7f988ecaf82f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/libc-start.c:291
Address 0x7ea500ed43b8 is a wild pointer inside of access range of size 0x000000000008.
SUMMARY: AddressSanitizer: use-after-poison (/mnt/scratch0/clusterfuzz/bot/builds/chrome-test-builds_media_linux-release_eb660d5ee526c9c1c1608a71fcbe7a713c490533/revisions/asan-linux-release-980233/chrome+0x1a4ed734) (BuildId: e7a6964bf90a878e)

Shadow bytes around the buggy address:
0x0fd5201d2820: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
0x0fd5201d2830: f7 f7 00 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7

```
  0x0fd5201d2830: f7 f7 00 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d2840: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d2850: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d2860: f7 f7 f7 f7 f7 00 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
=>0x0fd5201d2870: f7 f7 f7 f7 f7 f7 f7[f7]f7 f7 f7 f7 f7 f7 00 f7
  0x0fd5201d2880: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d2890: f7 f7 f7 f7 f7 f7 00 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d28a0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d28b0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd5201d28c0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==1==ABORTING
```

Did this work before? N/A

Chrome version: 99.0.4844.0 Channel: n/a
OS Version: 10.0

clusterfuzz-testcase-6544221896769536.zip
154 KB Download

asan.txt
5.9 KB View Download

Comment 1 by sheriffbot on Sat, Mar 12, 2022, 10:35 PM EST

Labels: external_security_report

Comment 2 by amyressler@chromium.org on Mon, Mar 14, 2022, 4:55 PM EDT

Labels: Restrict-View-SecurityEmbargo

setting RV-SE at reporting researcher's request

Comment 3 by bookholt@chromium.org on Mon, Mar 14, 2022, 6:12 PM EDT

Status: Assigned (was: Unconfirmed)

Owner: kron@chromium.org
Cc: hbos@chromium.org hta@chromium.org orphis@chromium.org steveanton@chromium.org tommi@chromium.org guidou@chromium.org
Labels: Security_Severity-High FoundIn-99 OS-Linux
Components: Blink>WebRTC>Perf

@kron, PTAL.

I'm not able to reproduce using the provided POC with a 99.0.4844.51 ASAN Linux build. However, PTAL due to potential for high severity security impact. The specific root cause analysis provided by the reporter should help reduce review energy.

Assigning severity High per history of UAF in sandboxed processes leading to RCE.

Comment 4 by sheriffbot on Mon, Mar 14, 2022, 6:14 PM EDT

Labels: Security_Impact-Stable

Comment 5 by m.coo...@gmail.com on Mon, Mar 14, 2022, 11:34 PM EDT

My fix is to invalidate the WeakPtrs of WebrtcVideoPerfReporter object when the PeerConnectionDependencyFactory object is about to be GCed.

```
diff --git a/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc
b/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc
index 7f756c5938..1335f5bfef 100644
--- a/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc
+++ b/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc
@@ -893,6 +893,7 @@ void PeerConnectionDependencyFactory::ContextDestroyed() {

 void PeerConnectionDependencyFactory::CleanupPeerConnectionFactory() {
   DVLOG(1) << "PeerConnectionDependencyFactory::CleanupPeerConnectionFactory()";
+  webrtc_video_perf_reporter_.Shutdown();
   socket_factory_ = nullptr;
   pc_factory_ = nullptr;
   if (network_manager_) {
diff --git a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
b/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
index 4b56ce341b..bd5ae201a1 100644
--- a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
+++ b/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
@@ -18,6 +18,10 @@ WebrtcVideoPerfReporter::~WebrtcVideoPerfReporter() {
   DCHECK(!task_runner_ || task_runner_->RunsTasksInCurrentSequence());
 }

+void WebrtcVideoPerfReporter::Shutdown(){
+  weak_factory_.InvalidateWeakPtrs();
+}
+
 void WebrtcVideoPerfReporter::Initialize(
     scoped_refptr<base::SingleThreadTaskRunner> task_runner,

     mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>
diff --git a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
b/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
```

```
b/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
index b353a48605..b48c3b341f 100644
--- a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
+++ b/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
@@ -32,6 +32,7 @@ class MODULES_EXPORT WebrtcVideoPerfReporter {
   void StoreWebrtcVideoStats(const StatsCollector::StatsKey& stats_key,
                              const StatsCollector::VideoStats& video_stats);

+  void Shutdown();
  private:
   void InitializeOnTaskRunner(
       mojo::PendingRemote<media::mojom::blink::WebrtcVideoPerfRecorder>

```

Fixpatch.diff
2.3 KB View Download

Comment 6 by kron@chromium.org on Tue, Mar 15, 2022, 11:57 AM EDT

I have not been able to reproduce this myself. I'm still waiting to get access to the clusterfuzz test.

The patch looks reasonable although I'm not convinced that the explanation in 3. is correct.

I've prepared a CL based on the patch in Comment #5 with some additions,
https://chromium-review.googlesource.com/c/chromium/src/+/3525393

Comment 7 by m.coo...@gmail.com on Tue, Mar 15, 2022, 12:13 PM EDT

re #c06
The test sample CF will be deleted after one week(Deletion: Will be auto-deleted on Sat, Mar 19, 2022 if flaky crash no longer seen),
if you need access to the CF report for confirmation, please contact the security team as soon as possible to associate the CF report with the issue

"The patch looks reasonable although I'm not convinced that the explanation in 3. is correct."

https://chromium.googlesource.com/chromium/src/+/67.0.3396.62/third_party/blink/renderer/platform/heap/BlinkGCDesign.md#sweeping-phase
Step 4-2. The thread invokes pre-finalizers. At this point, no destructors have been invoked. Thus the pre-finalizers are allowed to touch any other on-heap objects (which may get destructed in this sweeping phase).

You can also add debug log observations at CleanupPeerConnectionFactory and WebrtcVideoPerfReporter destructor.

Comment 8 by sheriffbot on Wed, Mar 16, 2022, 12:47 PM EDT

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 9 by sheriffbot on Wed, Mar 16, 2022, 1:07 PM EDT

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 10 by Git Watcher on Wed, Mar 16, 2022, 7:22 PM EDT

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7b04461342e737c2ff8d76bac719265bc84eda5a

commit 7b04461342e737c2ff8d76bac719265bc84eda5a
Author: Johannes Kron <kron@chromium.org>
Date: Wed Mar 16 23:21:55 2022

Force clean up before destruction of WebrtcVideoPerfReporter

~~Fixed: chromium:1305776~~
Change-Id: Iac432821447269fb78fb076bd1345157a5e928bf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3525393
Reviewed-by: Henrik Boström <hbos@chromium.org>
Commit-Queue: Johannes Kron <kron@chromium.org>
Cr-Commit-Position: refs/heads/main@{#981896}

[modify]
https://crrev.com/7b04461342e737c2ff8d76bac719265bc84eda5a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
[modify]
https://crrev.com/7b04461342e737c2ff8d76bac719265bc84eda5a/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
[modify]
https://crrev.com/7b04461342e737c2ff8d76bac719265bc84eda5a/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc

Comment 11 by sheriffbot on Thu, Mar 17, 2022, 12:42 PM EDT

Labels: reward-topanel

Comment 12 by sheriffbot on Thu, Mar 17, 2022, 1:37 PM EDT

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotifyWebRTC

Comment 13 by sheriffbot on Thu, Mar 17, 2022, 2:08 PM EDT

Labels: Merge-Request-100 Merge-Request-99

Requesting merge to stable M99 because latest trunk commit (981896) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (981896) appears to be after beta branch point (972766).

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

Comment 14 by amyressler@chromium.org on Thu, Mar 17, 2022, 3:12 PM EDT

Labels: -Merge-Request-99 merge-na-99

since this fix just landed < 24 hours ago, let's get this a bit more bake time in canary

in the meantime, merge-na-99 as there are not further planned releases of M99 stable

Comment 15 by sheriffbot on Thu, Mar 17, 2022, 7:24 PM EDT

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

Merge review required: M100 is already shipping to beta.

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

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 16 by amyressler@chromium.org on Mon, Mar 21, 2022, 2:28 PM EDT

Labels: -Merge-Review-100 Merge-Approved-100

M100 merge approved, please merge this fix into branch 4896 ASAP / NLT 3pm PDT today so this fix can be included in M100 stable cut

Comment 17 by srinivassista@google.com on Mon, Mar 21, 2022, 6:16 PM EDT

I have CP'ed to M100 here and run it through dry-run CQ,

https://chromium-review.googlesource.com/c/chromium/src/+/3540973

Please help land it asap. kron@

Comment 18 by Git Watcher on Mon, Mar 21, 2022, 7:36 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/+/140afbd23488af71aa535ce88e04c71ff772acf6

commit 140afbd23488af71aa535ce88e04c71ff772acf6
Author: Johannes Kron <kron@chromium.org>
Date: Mon Mar 21 23:35:04 2022

Force clean up before destruction of WebrtcVideoPerfReporter

(cherry picked from commit 7b04461342e737c2ff8d76bac719265bc84eda5a)

Fixed: chromium:1305776

~~Fixed: chromium:1305776~~
Change-Id: Iac432821447269fb78fb076bd1345157a5e928bf
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3525393
Reviewed-by: Henrik Boström <hbos@chromium.org>
Commit-Queue: Johannes Kron <kron@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#981896}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3540973
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Johannes Kron <kron@chromium.org>
Commit-Queue: Srinivas Sista <srinivassista@chromium.org>
Owners-Override: Srinivas Sista <srinivassista@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#764}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/140afbd23488af71aa535ce88e04c71ff772acf6/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.cc
[modify]
https://crrev.com/140afbd23488af71aa535ce88e04c71ff772acf6/third_party/blink/renderer/modules/peerconnection/webrtc_video_perf_reporter.h
[modify]
https://crrev.com/140afbd23488af71aa535ce88e04c71ff772acf6/third_party/blink/renderer/modules/peerconnection/peer_connection_dependency_factory.cc

Comment 19 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:31 PM EDT

Labels: Release-0-M100

Comment 20 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT

Labels: CVE-2022-1133 CVE_description-missing

Comment 21 by amyressler@google.com on Thu, Mar 31, 2022, 5:14 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 22 Deleted

Comment 23 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:26 PM EDT

(deleted the above comment as I conflated two separate responses into one)

Congratulations! The VRP Panel has decided to award you $5,000 for this report + $1,000 patch bonus. Thank you for all

Congratulations! The VRP Panel has decided to award you $5,000 for this report + $1,000 patch bonus. Thank you for all your efforts from the reporting of this bug and the extra analysis from RCA through to the fix.

(as discussed off bug, removing the RV-SE label -- please feel free to reach out directly if this is an issue)

Comment 24 by amyressler@google.com on Fri, Apr 1, 2022, 3:57 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 25 by sheriffbot on Thu, Jun 23, 2022, 1:31 PM EDT

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 26 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 27 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT

Labels: -CVE_description-missing --CVE_description-missing