Starred by 3 users

Owner: enga@chromium.org

CC: kbr@chromium.org
rzanoni@google.com
cwallez@chromium.org
bajones@chromium.org
amyressler@chromium.org
kainino@chromium.org
dsinclair@chromium.org

Status: Fixed *(Closed)*

Components: Blink>WebGPU
Internals>GPU>Dawn

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac, Lacros

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
M-100
Security_Severity-High
allpublic
CVE_description-submitted
Target-100
FoundIn-99
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1483

BlockedOn: ~~Issue 1315260~~
View details

Issue 1314754: Security: Missing bounds check in WebGPUDecoderImpl::DoRequestDevice

Reported by markbrand@google.com on Fri, Apr 8, 2022, 11:50 AM EDT Project Member

Code

VULNERABILITY DETAILS

There's a missing bounds check in WebGPUDecoderImpl:

```
void WebGPUDecoderImpl::DoRequestDevice(
    DawnRequestDeviceSerial request_device_serial,
    int32_t requested_adapter_index,
    uint32_t device_id,
    uint32_t device_generation,
    const WGPUDeviceProperties& request_device_properties) {
  // requested_adapter_index came from command buffer, these are actually
  // necessary bounds-checks and should not be DCHECKS.
  DCHECK_LE(0, requested_adapter_index);
  DCHECK_LT(static_cast<size_t>(requested_adapter_index),
            dawn_adapters_.size());

  // ... snip ...

  // Always enable "multi-planar-formats" as long as available.
  if (dawn_adapters_[requested_adapter_index] // dawn_adapters_ is an std::vector
          .GetAdapterProperties()
          .multiPlanarFormats) {
    required_features.push_back(WGPUFeatureName_DawnMultiPlanarFormats);
  }

  // ... snip ...

  dawn_adapters_[requested_adapter_index].RequestDevice(
      &device_descriptor,
      [](WGPURequestDeviceStatus status, WGPUDevice wgpu_device,
         const char* message, void* userdata) {
        std::unique_ptr<CallbackT> callback;
        callback.reset(static_cast<CallbackT*>(userdata));
        std::move(*callback).Run(status, wgpu_device, message);
      },
      new CallbackT(std::move(callback)));
}
```

dawn_adapters_ is effectively a vector of pointers to dawn::AdapterBase objects
and it looks like the second use of the out-of-bounds object will make a
virtual call through that pointer as long as some conditions are met.

https://source.chromium.org/chromium/chromium/src/+/main:third_party/dawn/src/dawn/native/Adapter.cpp;drc=5630be48e70e6de3514eb1f1e44c235bbec41d09;l=211

The attached PoC requires a renderer patch:

```
diff --git a/gpu/command_buffer/client/webgpu_implementation.cc b/gpu/command_buffer/client/webgpu_implementation.cc
index 696e4ec53538e..da0ce204f603e 100644
--- a/gpu/command_buffer/client/webgpu_implementation.cc
+++ b/gpu/command_buffer/client/webgpu_implementation.cc
@@ -630,7 +630,7 @@ void WebGPUImplementation::RequestDeviceAsync(
   dawn::wire::SerializeWGPUDeviceProperties(
       &requested_device_properties, reinterpret_cast<char*>(buffer.address()));

-  helper_->RequestDevice(request_device_serial, requested_adapter_id,
+  helper_->RequestDevice(request_device_serial, 0x4141,//requested_adapter_id,
                          reservation.id, reservation.generation,
                          buffer.shm_id(), buffer.offset(),
                          serialized_device_properties_size);
```

It's slightly painful to interact with the GPU process, so I don't have a PoC that doesn't require enabling WebGPU yet. (EnableUnsafeWebGPU, although I'm not convinced that this is a requirement).

This bug is subject to a 90-day disclosure deadline. If a fix for this issue is made available to users before the end of the 90-day deadline, this bug report will become public 30 days after the fix was made available. Otherwise, this bug report will become public at the deadline. The scheduled deadline is 2022-Jul-07.

VERSION
Chrome Version: stable
Operating System: tested on linux with --enable-features=Vulkan, but it should affect all platforms which support WebGPU.

REPRODUCTION CASE
Please include a demonstration of the security bug, such as an attached HTML or binary file that reproduces the bug when loaded in Chrome. PLEASE make the file as small as possible and remove any content not required to demonstrate the bug, or any personal or confidential information.

Please attach files directly, not in zip or other archive formats, and if you've created a demonstration site please also attach the files needed to reproduce the demonstration locally.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: GPU process
Crash State:

```
=================================================================
==2007==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6020000c8100 at pc 0x5593418ed38b bp
0x7ffd9165c5e0 sp 0x7ffd9165c5d8
READ of size 8 at 0x6020000c8100 thread T0 (chrome)
==2007==WARNING: invalid path to external symbolizer!
==2007==WARNING: Failed to use and restart external symbolizer!
    #0 0x5593418ed38a in dawn::native::Adapter::RequestDevice(WGPUDeviceDescriptor const*, void (*)

(WGPURequestDeviceStatus, WGPUDeviceImpl*, char const*, void*), void*)
./../../third_party/dawn/src/dawn/native/DawnNative.cpp:174:9
    #1 0x5593442bd198 in gpu::webgpu::WebGPUDecoderImpl::DoRequestDevice(unsigned long, int, unsigned int, unsigned
```

#1 0x5593442bd198 in gpu::webgpu::WebGPUDecoderImpl::DoRequestDevice(unsigned long, int, unsigned int, unsigned int, WGPUDeviceProperties const&) ./../../gpu/command_buffer/service/webgpu_decoder_impl.cc:1141:43
#2 0x5593442b7f78 in gpu::webgpu::WebGPUDecoderImpl::HandleRequestDevice(unsigned int, void const volatile*) ./../../gpu/command_buffer/service/webgpu_decoder_impl.cc:1607:3
#3 0x5593442bf1e4 in gpu::webgpu::WebGPUDecoderImpl::DoCommands(unsigned int, void const volatile*, int, int*) ./../../gpu/command_buffer/service/webgpu_decoder_impl.cc:1408:18
#4 0x5593441f1ff1 in gpu::CommandBufferService::Flush(int, gpu::AsyncAPIInterface*) ./../../gpu/command_buffer/service/command_buffer_service.cc:70:18
#5 0x5593441e279b in gpu::CommandBufferStub::OnAsyncFlush(int, unsigned int, std::__1::vector<gpu::SyncToken, std::__1::allocator<gpu::SyncToken> > const&) ./../../gpu/ipc/service/command_buffer_stub.cc:500:22
#6 0x5593441e1ce8 in gpu::CommandBufferStub::ExecuteDeferredRequest(gpu::mojom::DeferredCommandBufferRequestParams&) ./../../gpu/ipc/service/command_buffer_stub.cc:152:7
#7 0x5593441fa2e5 in gpu::GpuChannel::ExecuteDeferredRequest(mojo::StructPtr<gpu::mojom::DeferredRequestParams>) ./../../gpu/ipc/service/gpu_channel.cc:670:13
#8 0x559344207b35 in void base::internal::FunctorTraits<void (gpu::GpuChannel::*)(mojo::StructPtr<gpu::mojom::DeferredRequestParams>), void>::Invoke<void (gpu::GpuChannel::*)(mojo::StructPtr<gpu::mojom::DeferredRequestParams>), base::WeakPtr<gpu::GpuChannel>, mojo::StructPtr<gpu::mojom::DeferredRequestParams> >(void (gpu::GpuChannel::*)(mojo::StructPtr<gpu::mojom::DeferredRequestParams>), base::WeakPtr<gpu::GpuChannel>&&, mojo::StructPtr<gpu::mojom::DeferredRequestParams>&&) ./../../base/bind_internal.h:542:12
#9 0x5593442078c8 in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)(mojo::StructPtr<gpu::mojom::DeferredRequestParams>), base::WeakPtr<gpu::GpuChannel>, mojo::StructPtr<gpu::mojom::DeferredRequestParams> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:726:5
#10 0x559342724693 in gpu::Scheduler::RunNextTask() ./../../base/callback.h:142:12
#11 0x5593427324b4 in base::internal::Invoker<base::internal::BindState<void (gpu::Scheduler::*)(), base::internal::UnretainedWrapper<gpu::Scheduler> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:542:12
#12 0x55933d063438 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) ./../../base/callback.h:142:12
#13 0x55933d0b1ba8 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/common/task_annotator.h:74:5
#14 0x55933d0b108a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:291:41
#15 0x55933d0b2b9c in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
#16 0x55933cf59efe in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) ./../../base/message_loop/message_pump_glib.cc:375:46
#17 0x7f47504f1cda in g_main_context_dispatch ??:0:0

0x6020000c8100 is located 0 bytes to the right of 16-byte region [0x6020000c80f0,0x6020000c8100)
allocated by thread T0 (chrome) here:
#0 0x55932bd6f34d in operator new(unsigned long) _asan_rtl_:3
#1 0x5593442c8ece in void std::__1::vector<dawn::native::Adapter, std::__1::allocator<dawn::native::Adapter> >::__push_back_slow_path<dawn::native::Adapter const&>(dawn::native::Adapter const&) ./../../buildtools/third_party/libc++/trunk/include/new:235:10
#2 0x5593442bb2d1 in gpu::webgpu::WebGPUDecoderImpl::DiscoverAdapters() ./../../buildtools/third_party/libc++/trunk/include/vector:0:9

#3 0x5593442bab8b in gpu::webgpu::WebGPUDecoderImpl::Initialize() ./../../gpu/command_buffer/service/webgpu_decoder_impl.cc:1043:3
#4 0x5593442b4d54 in gpu::WebGPUCommandBufferStub::Initialize(gpu::CommandBufferStub*

#4 0x5593442b4d54 in gpu::WebGPUCommandBufferStub::Initialize(gpu::CommandBufferStub*,
gpu::mojom::CreateCommandBufferParams const&, base::UnsafeSharedMemoryRegion)
./../../gpu/ipc/service/webgpu_command_buffer_stub.cc:130:21
#5 0x5593441fd631 in
gpu::GpuChannel::CreateCommandBuffer(mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int,
base::UnsafeSharedMemoryRegion, mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>) ./../../gpu/ipc/service/gpu_channel.cc:890:13
#6 0x55934420a2bc in void base::internal::FunctorTraits<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int, base::UnsafeSharedMemoryRegion,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>), void>::Invoke<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int, base::UnsafeSharedMemoryRegion,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>), base::WeakPtr<gpu::GpuChannel>,
mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int, base::UnsafeSharedMemoryRegion,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)> >(void (gpu::GpuChannel::*)(mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int,
base::UnsafeSharedMemoryRegion, mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>), base::WeakPtr<gpu::GpuChannel>&&,
mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>&&, int&&, base::UnsafeSharedMemoryRegion&&,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>&&,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>&&, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>&&) ./../../base/bind_internal.h:542:12
#7 0x559344209f2b in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int, base::UnsafeSharedMemoryRegion,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)>), base::WeakPtr<gpu::GpuChannel>,
mojo::StructPtr<gpu::mojom::CreateCommandBufferParams>, int, base::UnsafeSharedMemoryRegion,
mojo::PendingAssociatedReceiver<gpu::mojom::CommandBuffer>,
mojo::PendingAssociatedRemote<gpu::mojom::CommandBufferClient>, base::OnceCallback<void (gpu::ContextResult,
gpu::Capabilities const&)> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:726:5
#8 0x55933d063438 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) ./../../base/callback.h:142:12
#9 0x55933d0b1ba8 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/common/task_annotator.h:74:5
#10 0x55933d0b108a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:291:41
#11 0x55933d0b2b9c in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
#12 0x55933cf58da4 in base::MessagePumpGlib::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_glib.cc:405:48
#13 0x55933d0b3474 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:498:12
#14 0x55933cff4285 in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:141:14

#15 0x55934a8a4077 in content::GpuMain(content::MainFunctionParams) ./../../content/gpu/gpu_main.cc:404:14
#16 0x55933bacdad1 in content::RunZygote(content::ContentMainDelegate*)
./../../content/app/content_main_runner_impl.cc:610:14

./../../content/app/content_main_runner_impl.cc:610:14
    #17 0x55933bacf716 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:692:12
    #18 0x55933bad217b in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1022:10
    #19 0x55933bac9e79 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*) ./../../content/app/content_main.cc:407:36
    #20 0x55933baca69e in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:435:10
    #21 0x55932bd71c09 in ChromeMain ./../../chrome/app/chrome_main.cc:176:12
    #22 0x55932bd71960 in main ./../../chrome/app/chrome_exe_main_aura.cc:17:10
    #23 0x7f474f3c87fc in __libc_start_main ./csu/../csu/libc-start.c:332:16

SUMMARY: AddressSanitizer: heap-buffer-overflow (/usr/local/google/home/markbrand/chromium/src/out/Asan/chrome+0x2a94538a) (BuildId: febd6058f01fa869)
Shadow bytes around the buggy address:
  0x0c0480010fd0: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c0480010fe0: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fd
  0x0c0480010ff0: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480011000: fa fa 00 00 fa fa fd fd fa fa fd fd fa fa fd fd
  0x0c0480011010: fa fa fd fa fa fa fd fd fa fa fd fa fa fa 00 00
=>0x0c0480011020:[fa]fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480011030: fa fa fd fa fa fa fd fd fa fa fd fa fa fa fd fa
  0x0c0480011040: fa fa 00 fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480011050: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480011060: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0c0480011070: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd 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
==2007==ABORTING

Client ID (if relevant): [see link above]

CREDIT INFORMATION

Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?

Reporter credit: Mark Brand of Google Project Zero

Reporter credit: Mark Brand of Google Project Zero

webgpu.html
223 bytes View Download

Comment 1 by rsesek@chromium.org on Fri, Apr 8, 2022, 4:06 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: enga@chromium.org
Cc: kbr@chromium.org bajones@chromium.org
Labels: Security_Severity-High FoundIn-99 OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Blink>WebGPU Internals>GPU>Dawn

Comment 2 by sheriffbot on Fri, Apr 8, 2022, 4:06 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 3 by sheriffbot on Sat, Apr 9, 2022, 12:46 PM EDT Project Member

Labels: M-100 Target-100

Setting milestone and target because of high severity.

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

Comment 4 by enga@chromium.org on Mon, Apr 11, 2022, 12:52 PM EDT Project Member

Cc: cwallez@chromium.org

I'll make a fix, and I'll follow-up with removing this custom manually-written serialization code. It's about time we've removed it to avoid this type of bug.

Comment 5 by enga@chromium.org on Mon, Apr 11, 2022, 1:04 PM EDT Project Member

Blockedon: 1315260

Comment 6 by markbrand@google.com on Tue, Apr 12, 2022, 8:54 AM EDT Project Member

FYI I've verified that this is reachable from a compromised renderer that isn't part of the Origin trial. (ie. tested on Linux with --enable-features=Vulkan,WebGPUService). As far as I understand that should match the current situation for official builds on the platforms that support GPU acceleration by default (WebGPUService feature enabled to 100% by finch).

I haven't uploaded a new PoC, since it requires a bit of messing around in the build to get working and it's less reliable than the original example so I don't think it's really useful for testing.

Comment 7 by Git Watcher on Tue, Apr 12, 2022, 10:32 AM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47

commit bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47
Author: Austin Eng <enga@chromium.org>

Date: Tue Apr 12 14:31:00 2022

Add bounds check to WebGPUDecoderImplDoRequestDevice

Add bounds check to WebGPUDecoderImpl::DoRequestDevice

~~Fixed: chromium:1314754~~
Change-Id: Id23af9cc3df08cca3ce7d627e3761c9a65a2c802
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3580555
Reviewed-by: Corentin Wallez <cwallez@chromium.org>
Commit-Queue: Austin Eng <enga@chromium.org>
Cr-Commit-Position: refs/heads/main@{#991510}

[modify]
https://crrev.com/bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47/gpu/command_buffer/service/webgpu_decoder_impl.cc

Comment 8 by enga@chromium.org on Tue, Apr 12, 2022, 1:16 PM EDT Project Member

Labels: Merge-Request-100 Merge-Request-101 Merge-Request-96

Comment 9 by sheriffbot on Tue, Apr 12, 2022, 1:40 PM EDT Project Member

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

Comment 10 by sheriffbot on Wed, Apr 13, 2022, 10:37 AM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: M101 is already shipping to beta.

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

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 11 by sheriffbot on Wed, Apr 13, 2022, 10:37 AM EDT Project Member

Labels: -Merge-Request-100 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?

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 12 by sheriffbot on Wed, Apr 13, 2022, 10:37 AM EDT Project Member

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

Merge review required: M96 is already shipping to stable.

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

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

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

Comment 13 by enga@chromium.org on Wed, Apr 13, 2022, 10:40 AM EDT Project Member

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

It is a Severity-High security bug

2. What changes specifically would you like to merge? Please link to Gerrit.
https://chromium-review.googlesource.com/c/chromium/src/+/3580555

3. Have the changes been released and tested on canary?

Yes, it is in Canary 102.0.5001.0
https://chromiumdash.appspot.com/commit/bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

The change is not a new feature. It is for a feature which is launched to 100% via Finch

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents

N/A

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.

No.

Comment 14 by amyressler@chromium.org on Fri, Apr 15, 2022, 8:26 PM EDT Project Member

Labels: -Merge-Review-96 -Merge-Review-100 -Merge-Review-101 Merge-Approved-100 Merge-Approved-101

M101 merge approved, please merge to branch 4951
M101 merge approved, please merge to branch 4896
please complete these merges asap/nlt noon PST 19 April (Tuesday) so these fixes can be included in the M101 stable and M100 extended release cuts

Comment 15 by Git Watcher on Mon, Apr 18, 2022, 1:22 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f935b27591ed2974f0a8471c85c0840b5ded5ce8

commit f935b27591ed2974f0a8471c85c0840b5ded5ce8
Author: Austin Eng <enga@chromium.org>
Date: Mon Apr 18 17:21:56 2022

Add bounds check to WebGPUDecoderImpl::DoRequestDevice

(cherry picked from commit bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47)

~~Fixed: chromium:1314754~~
Change-Id: Id23af9cc3df08cca3ce7d627e3761c9a65a2c802
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3580555
Reviewed-by: Corentin Wallez <cwallez@chromium.org>
Commit-Queue: Austin Eng <enga@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#991510}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3590652
Auto-Submit: Austin Eng <enga@chromium.org>
Reviewed-by: Brandon Jones <bajones@chromium.org>
Commit-Queue: Brandon Jones <bajones@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#847}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/f935b27591ed2974f0a8471c85c0840b5ded5ce8/gpu/command_buffer/service/webgpu_decoder_impl.cc

Comment 16 by sheriffbot on Mon, Apr 18, 2022, 1:22 PM EDT Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?

1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 17 by rzanoni@google.com on Mon, Apr 18, 2022, 1:39 PM EDT Project Member

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 18 by rzanoni@google.com on Mon, Apr 18, 2022, 3:31 PM EDT Project Member

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 19 by sheriffbot on Mon, Apr 18, 2022, 3:31 PM EDT Project Member

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

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 20 by rzanoni@google.com on Mon, Apr 18, 2022, 3:38 PM EDT Project Member

1. Just https://crrev.com/c/3589810
2. Low conflicts
3. 100, 101
4. Yes

Comment 21 by gmpritchard@google.com on Tue, Apr 19, 2022, 11:14 AM EDT Project Member

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

Comment 22 by enga@chromium.org on Tue, Apr 19, 2022, 11:15 AM EDT Project Member

m100 CQ is broken
looks like several CLs have been submitted manually like https://chromium-review.googlesource.com/c/chromium/src/+/3564640

https://chromium-review.googlesource.com/c/chromium/src/+/3590406 passed all tests except for the broken ones on this builder:
https://ci.chromium.org/p/chromium-m100/builders/try/win_optional_gpu_tests_rel. can I manually submit it?

Comment 23 by sheriffbot on Tue, Apr 19, 2022, 12:19 PM EDT Project Member

Cc: amyressler@chromium.org

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 24 by Git Watcher on Wed, Apr 20, 2022, 3:48 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/80fda5a57b7540dd972a4233bc20316d9a65754f

commit 80fda5a57b7540dd972a4233bc20316d9a65754f
Author: Austin Eng <enga@chromium.org>
Date: Wed Apr 20 19:46:58 2022

Add bounds check to WebGPUDecoderImpl::DoRequestDevice

(cherry picked from commit bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47)

~~Fixed: chromium:1314754~~
Change-Id: Id23af9cc3df08cca3ce7d627e3761c9a65a2c802
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3580555
Reviewed-by: Corentin Wallez <cwallez@chromium.org>
Commit-Queue: Austin Eng <enga@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#991510}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3590406
Auto-Submit: Austin Eng <enga@chromium.org>
Reviewed-by: Brandon Jones <bajones@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#1164}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/80fda5a57b7540dd972a4233bc20316d9a65754f/gpu/command_buffer/service/webgpu_decoder_impl.cc

Comment 25 by gmpritchard@google.com on Fri, Apr 22, 2022, 12:10 PM EDT Project Member

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 26 by amyressler@chromium.org on Mon, Apr 25, 2022, 12:45 PM EDT Project Member

Labels: Release-0-M101

Comment 27 by Git Watcher on Mon, Apr 25, 2022, 5:02 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5361d836aeb1bde7fb3ef333209a65b61e1911fe

commit 5361d836aeb1bde7fb3ef333209a65b61e1911fe
Author: Austin Eng <enga@chromium.org>
Date: Mon Apr 25 21:01:40 2022

Date: Mon Apr 25 21:01:40 2022

[M96-LTS] Add bounds check to WebGPUDecoderImpl::DoRequestDevice

(cherry picked from commit bee4701c99cbbbb25c0bd6c5c79a40f63f1b1e47)

~~Fixed: chromium:1314754~~
Change-Id: Id23af9cc3df08cca3ce7d627e3761c9a65a2c802
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3580555
Commit-Queue: Austin Eng <enga@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#991510}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3589810
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1603}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/5361d836aeb1bde7fb3ef333209a65b61e1911fe/gpu/command_buffer/service/webgpu_decoder_impl.cc

Comment 28 by rzanoni@google.com on Tue, Apr 26, 2022, 9:39 AM EDT Project Member

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 29 by amyressler@google.com on Tue, Apr 26, 2022, 4:31 PM EDT Project Member

Labels: CVE-2022-1483 CVE_description-missing

Comment 30 by sheriffbot on Wed, Jul 20, 2022, 1:32 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

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

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

Comment 31 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 32 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing