Starred by 3 users

Owner:	jmad...@chromium.org
CC:	rzanoni@google.com cclao@google.com
Status:	Fixed *(Closed)*
Components:	Internals>GPU>ANGLE
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-98
reward-7000
Target-98
FoundIn-96
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
LTS-Merge-Merged-96
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0978

Issue 1299264: use after free in rx::FramebufferVk::startNewRenderPass

Reported by emily...@gmail.com on Sun, Feb 20, 2022, 10:06 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36

Steps to reproduce the problem:
tested os:
ubuntu 20.04
tested chrome version:
Version 99.0.4844.11 (Official Build) dev (64-bit)
Chromium 100.0.4880.0(gs://chromium-browser-asan/linux-release/asan-linux-release-973350.zip)

./chrome http://localhost:8605/crash.html

What is the expected behavior?

What went wrong?
==2698179==ERROR: AddressSanitizer: heap-use-after-free on address 0x6060002c1354 at pc 0x7f1ff61702a1 bp 0x7ffc915916d0 sp 0x7ffc915916c8
READ of size 4 at 0x6060002c1354 thread T0 (chrome)
    #0 0x7f1ff61702a0 in isImageTransient ./../../third_party/angle/src/libANGLE/renderer/vulkan/RenderTargetVk.h:135:44
    #1 0x7f1ff61702a0 in rx::FramebufferVk::startNewRenderPass(rx::ContextVk*, gl::RectangleImpl<int> const&, rx::vk::priv::SecondaryCommandBuffer**, bool*) ./../../third_party/angle/src/libANGLE/renderer/vulkan/FramebufferVk.cpp:2439:66
    #2 0x7f1ff612558e in rx::ContextVk::startRenderPass(gl::RectangleImpl<int>, rx::vk::priv::SecondaryCommandBuffer**, bool*) ./../../third_party/angle/src/libANGLE/renderer/vulkan/ContextVk.cpp:6000:5
    #3 0x7f1ff6110be6 in rx::ContextVk::handleDirtyGraphicsRenderPass(angle::BitSetT<18ul, unsigned long, unsigned long>::Iterator*, angle::BitSetT<18ul, unsigned long, unsigned long>) ./../../third_party/angle/src/libANGLE/renderer/vulkan/ContextVk.cpp:1735:5
    #4 0x7f1ff611e899 in rx::ContextVk::setupDraw(gl::Context const*, gl::PrimitiveMode, int, int, int, gl::DrawElementsType, void const*, angle::BitSetT<18ul, unsigned long, unsigned long>) ./../../third_party/angle/src/libANGLE/renderer/vulkan/ContextVk.cpp:1188:9
    #5 0x7f1ff6128ce1 in rx::ContextVk::drawArrays(gl::Context const*, gl::PrimitiveMode, int, int) ./../../third_party/angle/src/libANGLE/renderer/vulkan/ContextVk.cpp:2737:9
    #6 0x7f1ff5a14c6c in drawArrays ./../../third_party/angle/src/libANGLE/Context.inl.h:133:5
    #7 0x7f1ff5a14c6c in GL_DrawArrays ./../../third_party/angle/src/libGLESv2/entry_points_gles_2_0_autogen.cpp:1109:22
    #8 0x560ef602fa65 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays(unsigned int, int, int) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough_doers.cc:1217:10
    #9 0x560ef5ffc850 in gpu::error::Error gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<false>(unsigned int, void const volatile*, int, int*) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough.cc:871:20
    #10 0x560ef64b2d05 in gpu::CommandBufferService::Flush(int, gpu::AsyncAPIInterface*) ./../../gpu/command_buffer/service/command_buffer_service.cc:70:18
    #11 0x560ef64a5f98 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:499:22
    #12 0x560ef64a5445 in

gpu::CommandBufferStub::ExecuteDeferredRequest(gpu::mojom::DeferredCommandBufferRequestParams&) ./../../gpu/ipc/service/command_buffer_stub.cc:151:7
    #13 0x560ef64b0d26 in

#13 0x560ef64b9d26 in
gpu::GpuChannel::ExecuteDeferredRequest(mojo::StructPtr<gpu::mojom::DeferredRequestParams>)
./../../gpu/ipc/service/gpu_channel.cc:669:13
#14 0x560ef64c71f2 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
#15 0x560ef4e02cec in Run ./../../base/callback.h:142:12
#16 0x560ef4e02cec in gpu::Scheduler::RunNextTask() ./../../gpu/command_buffer/service/scheduler.cc:684:26
#17 0x560ef023899f in Run ./../../base/callback.h:142:12
#18 0x560ef023899f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
#19 0x560ef027dd57 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:389:29)>
./../../base/task/common/task_annotator.h:74:5
#20 0x560ef027dd57 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:21
#21 0x560ef027d42f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:292:41
#22 0x560ef027ea27 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
#23 0x560ef012ea55 in HandleDispatch ./../../base/message_loop/message_pump_glib.cc:375:46
#24 0x560ef012ea55 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*)
./../../base/message_loop/message_pump_glib.cc:126:43
#25 0x7f1fff56317c in g_main_context_dispatch ??:0:0

0x6060002c1354 is located 52 bytes inside of 56-byte region [0x6060002c1320,0x6060002c1358)
freed by thread T0 (chrome) here:
#0 0x560ee17988cd in operator delete(void*) _asan_rtl_:3
#1 0x7f1ff6224d99 in __libcpp_operator_delete<void *> ./../../buildtools/third_party/libc++/trunk/include/new:245:3
#2 0x7f1ff6224d99 in __do_deallocate_handle_size<> ./../../buildtools/third_party/libc++/trunk/include/new:269:10
#3 0x7f1ff6224d99 in __libcpp_deallocate ./../../buildtools/third_party/libc++/trunk/include/new:279:12
#4 0x7f1ff6224d99 in deallocate ./../../buildtools/third_party/libc++/trunk/include/__memory/allocator.h:91:13
#5 0x7f1ff6224d99 in deallocate ./../../buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:281:13
#6 0x7f1ff6224d99 in ~__vector_base ./../../buildtools/third_party/libc++/trunk/include/vector:467:9
#7 0x7f1ff6224d99 in ~vector ./../../buildtools/third_party/libc++/trunk/include/vector:558:5
#8 0x7f1ff6224d99 in destroy ./../../buildtools/third_party/libc++/trunk/include/__memory/allocator.h:133:15
#9 0x7f1ff6224d99 in destroy<std::__1::vector<rx::RenderTargetVk, std::__1::allocator<rx::RenderTargetVk> >, void>
./../../buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:308:13
#10 0x7f1ff6224d99 in __destruct_at_end ./../../buildtools/third_party/libc++/trunk/include/vector:429:9
#11 0x7f1ff6224d99 in std::__1::__vector_base<std::__1::vector<rx::RenderTargetVk,
std::__1::allocator<rx::RenderTargetVk> >, std::__1::allocator<std::__1::vector<rx::RenderTargetVk,
std::__1::allocator<rx::RenderTargetVk> > > >::clear() ./../../buildtools/third_party/libc++/trunk/include/vector:372:29
#12 0x7f1ff6216327 in clear ./../../buildtools/third_party/libc++/trunk/include/vector:775:17
#13 0x7f1ff6216327 in rx::TextureVk::releaseImage(rx::ContextVk*)
./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:3062:23
#14 0x7f1ff621c8b5 in rx::TextureVk::respecifyImageStorage(rx::ContextVk*)

./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2264:9
#15 0x7f1ff621bfeb in rx::TextureVk::maybeUpdateBaseMaxLevels(rx::ContextVk*, bool*)
./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2006:9

./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2006:9
    #16 0x7f1ff6221542 in rx::TextureVk::syncState(gl::Context const*, angle::BitSetT<24ul, unsigned long, unsigned long> const&, gl::Command) ./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2636:5
    #17 0x7f1ff5c991e3 in gl::Texture::syncState(gl::Context const*, gl::Command) ./../../third_party/angle/src/libANGLE/Texture.cpp:2125:5
    #18 0x7f1ff5c77bd4 in gl::State::syncTextures(gl::Context const*, gl::Command) ./../../third_party/angle/src/libANGLE/State.cpp:3390:13
    #19 0x7f1ff5a14b49 in syncDirtyObjects ./../../third_party/angle/src/libANGLE/State.h:1178:9
    #20 0x7f1ff5a14b49 in syncDirtyObjects ./../../third_party/angle/src/libANGLE/Context.inl.h:107:19
    #21 0x7f1ff5a14b49 in prepareForDraw ./../../third_party/angle/src/libANGLE/Context.inl.h:117:5
    #22 0x7f1ff5a14b49 in drawArrays ./../../third_party/angle/src/libANGLE/Context.inl.h:132:5
    #23 0x7f1ff5a14b49 in GL_DrawArrays ./../../third_party/angle/src/libGLESv2/entry_points_gles_2_0_autogen.cpp:1109:22
    #24 0x560ef602fa65 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays(unsigned int, int, int) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough_doers.cc:1217:10
    #25 0x560ef5ffc850 in gpu::error::Error gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<false>(unsigned int, void const volatile*, int, int*) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough.cc:871:20
    #26 0x560ef64b2d05 in gpu::CommandBufferService::Flush(int, gpu::AsyncAPIInterface*) ./../../gpu/command_buffer/service/command_buffer_service.cc:70:18
    #27 0x560ef64a5f98 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:499:22
    #28 0x560ef64a5445 in gpu::CommandBufferStub::ExecuteDeferredRequest(gpu::mojom::DeferredCommandBufferRequestParams&) ./../../gpu/ipc/service/command_buffer_stub.cc:151:7
    #29 0x560ef64b9d26 in gpu::GpuChannel::ExecuteDeferredRequest(mojo::StructPtr<gpu::mojom::DeferredRequestParams>) ./../../gpu/ipc/service/gpu_channel.cc:669:13
    #30 0x560ef64c71f2 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
    #31 0x560ef4e02cec in Run ./../../base/callback.h:142:12
    #32 0x560ef4e02cec in gpu::Scheduler::RunNextTask() ./../../gpu/command_buffer/service/scheduler.cc:684:26
    #33 0x560ef023899f in Run ./../../base/callback.h:142:12
    #34 0x560ef023899f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) ./../../base/task/common/task_annotator.cc:135:32
    #35 0x560ef027dd57 in RunTask<(lambda at ../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:389:29)> ./../../base/task/common/task_annotator.h:74:5
    #36 0x560ef027dd57 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:21
    #37 0x560ef027d42f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:292:41
    #38 0x560ef027ea27 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #39 0x560ef012ea55 in HandleDispatch ./../../base/message_loop/message_pump_glib.cc:375:46
    #40 0x560ef012ea55 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) ./../../base/message_loop/message_pump_glib.cc:126:43

    #41 0x7f1fff56317c in g_main_context_dispatch ??:0:0

previously allocated by thread T0 (chrome) here:

previously allocated by thread T0 (chrome) here:
#0 0x560ee179806d in operator new(unsigned long) _asan_rtl_:3
#1 0x7f1ff6225c68 in __libcpp_operator_new<unsigned long> ./../../buildtools/third_party/libc++/trunk/include/new:235:10
#2 0x7f1ff6225c68 in __libcpp_allocate ./../../buildtools/third_party/libc++/trunk/include/new:261:10
#3 0x7f1ff6225c68 in allocate ./../../buildtools/third_party/libc++/trunk/include/__memory/allocator.h:82:38
#4 0x7f1ff6225c68 in allocate ./../../buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:261:20
#5 0x7f1ff6225c68 in __split_buffer ./../../buildtools/third_party/libc++/trunk/include/__split_buffer:314:29
#6 0x7f1ff6225c68 in std::__1::vector<rx::RenderTargetVk, std::__1::allocator<rx::RenderTargetVk> >::__append(unsigned long) ./../../buildtools/third_party/libc++/trunk/include/vector:1094:53
#7 0x7f1ff6220365 in resize ./../../buildtools/third_party/libc++/trunk/include/vector:2025:15
#8 0x7f1ff6220365 in rx::TextureVk::initSingleLayerRenderTargets(rx::ContextVk*, unsigned int, gl::LevelIndexWrapper<int>, gl::RenderToTextureImageIndex) ./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2444:19
#9 0x7f1ff621ff82 in rx::TextureVk::getAttachmentRenderTarget(gl::Context const*, unsigned int, gl::ImageIndex const&, int, rx::FramebufferAttachmentRenderTarget**) ./../../third_party/angle/src/libANGLE/renderer/vulkan/TextureVk.cpp:2364:9
#10 0x7f1ff616cafa in getRenderTargetImpl ./../../third_party/angle/src/libANGLE/FramebufferAttachment.h:277:23
#11 0x7f1ff616cafa in getRenderTarget<rx::RenderTargetVk> ./../../third_party/angle/src/libANGLE/FramebufferAttachment.h:151:16
#12 0x7f1ff616cafa in updateCachedRenderTarget ./../../third_party/angle/src/libANGLE/renderer/RenderTargetCache.h:163:9
#13 0x7f1ff616cafa in updateReadColorRenderTarget ./../../third_party/angle/src/libANGLE/renderer/RenderTargetCache.h:124:12
#14 0x7f1ff616cafa in rx::RenderTargetCache<rx::RenderTargetVk>::updateColorRenderTarget(gl::Context const*, gl::FramebufferState const&, unsigned long) ./../../third_party/angle/src/libANGLE/renderer/RenderTargetCache.h:137:9
#15 0x7f1ff616c527 in rx::FramebufferVk::updateColorAttachment(gl::Context const*, unsigned int) ./../../third_party/angle/src/libANGLE/renderer/vulkan/FramebufferVk.cpp:1645:5
#16 0x7f1ff616d4bf in rx::FramebufferVk::syncState(gl::Context const*, unsigned int, angle::BitSetT<29ul, unsigned long, unsigned long> const&, gl::Command) ./../../third_party/angle/src/libANGLE/renderer/vulkan/FramebufferVk.cpp:1866:17
#17 0x7f1ff5b4cde4 in gl::Framebuffer::syncState(gl::Context const*, unsigned int, gl::Command) const ./../../third_party/angle/src/libANGLE/Framebuffer.cpp:2061:9
#18 0x7f1ff5a14b49 in syncDirtyObjects ./../../third_party/angle/src/libANGLE/State.h:1178:9
#19 0x7f1ff5a14b49 in syncDirtyObjects ./../../third_party/angle/src/libANGLE/Context.inl.h:107:19
#20 0x7f1ff5a14b49 in prepareForDraw ./../../third_party/angle/src/libANGLE/Context.inl.h:117:5
#21 0x7f1ff5a14b49 in drawArrays ./../../third_party/angle/src/libANGLE/Context.inl.h:132:5
#22 0x7f1ff5a14b49 in GL_DrawArrays ./../../third_party/angle/src/libGLESv2/entry_points_gles_2_0_autogen.cpp:1109:22
#23 0x560ef602fa65 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays(unsigned int, int, int) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough_doers.cc:1217:10
#24 0x560ef5ffc850 in gpu::error::Error gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<false>(unsigned int, void const volatile*, int, int*) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough.cc:871:20
#25 0x560ef64b2d05 in gpu::CommandBufferService::Flush(int, gpu::AsyncAPIInterface*) ./../../gpu/command_buffer/service/command_buffer_service.cc:70:18
#26 0x560ef64a5f98 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:499:22
#27 0x560ef64a5445 in gpu::CommandBufferStub::ExecuteDeferredRequest(gpu::mojom::DeferredCommandBufferRequestParams&) ./../../gpu/ipc/service/command_buffer_stub.cc:151:7
#28 0x560ef64b9d26 in gpu::GpuChannel::ExecuteDeferredRequest(mojo::StructPtr<gpu::mojom::DeferredRequestParams>) ./../../gpu/ipc/service/gpu_channel.cc:669:13
#29 0x560ef64c71f2 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
    #30 0x560ef4e02cec in Run ./../../base/callback.h:142:12
    #31 0x560ef4e02cec in gpu::Scheduler::RunNextTask() ./../../gpu/command_buffer/service/scheduler.cc:684:26
    #32 0x560ef023899f in Run ./../../base/callback.h:142:12
    #33 0x560ef023899f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
    #34 0x560ef027dd57 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:389:29)>
./../../base/task/common/task_annotator.h:74:5
    #35 0x560ef027dd57 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:21
    #36 0x560ef027d42f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:292:41
    #37 0x560ef027ea27 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #38 0x560ef012ea55 in HandleDispatch ./../../base/message_loop/message_pump_glib.cc:375:46
    #39 0x560ef012ea55 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*)
./../../base/message_loop/message_pump_glib.cc:126:43
    #40 0x7f1fff56317c in g_main_context_dispatch ??:0:0

SUMMARY: AddressSanitizer: heap-use-after-free
(/home/exp11/chromium/src/out/chrome_asan_shared/libGLESv2.so+0xec72a0) (BuildId: c0952d059579718e)
Shadow bytes around the buggy address:
  0x0c0c80050210: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c0c80050220: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c80050230: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c80050240: fd fd fd fd fd fd fd fd fa fa fa fa 00 00 00 00
  0x0c0c80050250: 00 00 fc fc fa fa fa fa 00 00 00 00 00 00 00 fa
=>0x0c0c80050260: fa fa fa fa fd fd fd fd fd[fd]fa fa fa fa fa
  0x0c0c80050270: 00 00 00 00 00 00 00 fa fa fa fa fa fd fd fd fd
  0x0c0c80050280: fd fd fd fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c0c80050290: fa fa fa fa fd fd fd fd fd fd fd fd fa fa fa fa
  0x0c0c800502a0: fd fd fd fd fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c0c800502b0: fd fd fd fd fa fa fa fa fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable: 00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone: fa
  Freed heap region: fd
  Stack left redzone: f1
  Stack mid redzone: f2
  Stack right redzone: f3
  Stack after return: f5
  Stack use after scope: f8
  Global redzone: f9
  Global init order: f6
  Poisoned by user: f7
  Container overflow: fc

  Array cookie: ac
  Intra object redzone: bb
  ASan internal: fe

```
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==2698179==ABORTING
Received signal 6
    #0 0x560ee17213ff in backtrace /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:4277:13
    #1 0x560ef0329264 in base::debug::CollectStackTrace(void**, unsigned long)
./../../base/debug/stack_trace_posix.cc:874:39
    #2 0x560ef00ce272 in StackTrace ./../../base/debug/stack_trace.cc:222:12
    #3 0x560ef00ce272 in base::debug::StackTrace::StackTrace() ./../../base/debug/stack_trace.cc:219:28
    #4 0x560ef0327cfe in base::debug::(anonymous namespace)::StackDumpSignalHandler(int, siginfo_t*, void*)
./../../base/debug/stack_trace_posix.cc:371:3
    #5 0x7f1fff6c7420 in __funlockfile :?
    #6 0x7f1ffe03915b in __libc_signal_restore_set /build/glibc-49eTd7/glibc-2.31/signal/../sysdeps/unix/sysv/linux/internal-
signals.h:86:3
    #7 0x7f1ffe03915b in raise /build/glibc-49eTd7/glibc-2.31/signal/../sysdeps/unix/sysv/linux/raise.c:48:3
    #8 0x7f1ffe018859 in abort /build/glibc-49eTd7/glibc-2.31/stdlib/abort.c:79:7
    #9 0x560ee1784167 in __sanitizer::Abort() /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/sanitizer_common/sanitizer_posix_libcdep.cpp:143:3
    #10 0x560ee1782a81 in __sanitizer::Die() /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-
rt/lib/sanitizer_common/sanitizer_termination.cpp:58:5
    #11 0x560ee176b5f7 in __asan::ScopedInErrorReport::~ScopedInErrorReport() _asan_rtl_:7
    #12 0x560ee176e26f in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool,
unsigned long, unsigned int, bool) _asan_rtl_:1
    #13 0x560ee176ee68 in __asan_report_load4 _asan_rtl_:1
#12 0x7f1ff61702a1 <unknown>
#13 0x7f1ff612558f <unknown>
#14 0x7f1ff6110be7 <unknown>
#15 0x7f1ff611e89a <unknown>
#16 0x7f1ff6128ce2 <unknown>
#17 0x7f1ff5a14c6d <unknown>
    #14 0x560ef602fa66 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays(unsigned int, int, int)
./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough_doers.cc:1217:10
    #15 0x560ef5ffc851 in gpu::error::Error gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<false>(unsigned
int, void const volatile*, int, int*) ./../../gpu/command_buffer/service/gles2_cmd_decoder_passthrough.cc:871:20
    #16 0x560ef64b2d06 in gpu::CommandBufferService::Flush(int, gpu::AsyncAPIInterface*)
./../../gpu/command_buffer/service/command_buffer_service.cc:70:18
    #17 0x560ef64a5f99 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:499:22
    #18 0x560ef64a5446 in
gpu::CommandBufferStub::ExecuteDeferredRequest(gpu::mojom::DeferredCommandBufferRequestParams&)
./../../gpu/ipc/service/command_buffer_stub.cc:151:7
    #19 0x560ef64b9d27 in
gpu::GpuChannel::ExecuteDeferredRequest(mojo::StructPtr<gpu::mojom::DeferredRequestParams>)
./../../gpu/ipc/service/gpu_channel.cc:669:13
    #20 0x560ef64c71f3 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
    #21 0x560ef4e02ced in Run ./../../base/callback.h:142:12
    #22 0x560ef4e02ced in gpu::Scheduler::RunNextTask() ./../../gpu/command_buffer/service/scheduler.cc:684:26
```

#22 0x560ef4e02ced in gpu::Scheduler::RunNextTask() ./../../gpu/command_buffer/service/scheduler.cc:684:26
#23 0x560ef02389a0 in Run ./../../base/callback.h:142:12
#24 0x560ef02389a0 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
#25 0x560ef027dd58 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:389:29)>
./../../base/task/common/task_annotator.h:74:5
#26 0x560ef027dd58 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:21
#27 0x560ef027d430 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:292:41
#28 0x560ef027ea28 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
#29 0x560ef012ea56 in HandleDispatch ./../../base/message_loop/message_pump_glib.cc:375:46
#30 0x560ef012ea56 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*)
./../../base/message_loop/message_pump_glib.cc:126:43
#31 0x7f1fff56317d in g_main_context_dispatch ??:0:0
#32 0x7f1fff563400 in g_main_context_dispatch ??:?
#33 0x7f1fff5634a3 in g_main_context_iteration ??:0:0
#34 0x560ef012dd2f in base::MessagePumpGlib::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_glib.cc:401:30
#35 0x560ef027f114 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:499:12
#36 0x560ef01b24d6 in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:141:14
#37 0x560efca36af4 in content::GpuMain(content::MainFunctionParams) ./../../content/gpu/gpu_main.cc:404:14
#38 0x560eeefa4f2e 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:683:14
#39 0x560eeefa6dbc in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1043:10
#40 0x560eeefa0864 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:399:36
#41 0x560eeefa0f49 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:427:10
#42 0x560ee179b013 in ChromeMain ./../../chrome/app/chrome_main.cc:176:12
#43 0x560ee179adb2 in main ./../../chrome/app/chrome_exe_main_aura.cc:17:10
#44 0x7f1ffe01a083 in __libc_start_main /build/glibc-49eTd7/glibc-2.31/csu/../csu/libc-start.c:308:16
#45 0x560ee16e7cea in _start ??:0:0
r8: 0000000000000000 r9: 00007ffc915906e0 r10: 0000000000000008 r11: 0000000000000246
r12: 10000000000fffff r13: 0fffff0000000000 r14: 1000000000000000 r15: 2000000000000000
di: 0000000000000002 si: 00007ffc915906e0 bp: 6000000000000000 bx: 00007f1ffd0c4e80
dx: 0000000000000000 ax: 0000000000000000 cx: 00007f1ffe03915b sp: 00007ffc915906e0
ip: 00007f1ffe03915b efl: 0000000000000246 cgf: 002b000000000033 erf: 0000000000000000
trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]
[2697920:2697920:0220/210825.473479:ERROR:gpu_process_host.cc(974)] GPU process exited unexpectedly:
exit_code=134
[2701709:2701709:0220/210825.685636:ERROR:sandbox_linux.cc(377)] InitializeSandbox() called with multiple threads in process gpu-process.

Did this work before? N/A

Chrome version: Version 99.0.4844.11 (Official Build) dev (64-bit) Channel: n/a
OS Version: 20.04

OS Version: 20.04

crash.html
1.9 KB View Download

Comment 1 by sheriffbot on Sun, Feb 20, 2022, 10:11 AM EST Project Member

Labels: external_security_report

Comment 2 by danakj@chromium.org on Tue, Feb 22, 2022, 5:49 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: jmad...@chromium.org
Labels: FoundIn-96 Security_Severity-Critical Pri-1
Components: Internals>GPU>ANGLE

I can repro in asan with --disable-gpu on M96

No sandbox in GPU process on android -> critical

Comment 3 by danakj@chromium.org on Tue, Feb 22, 2022, 5:49 PM EST Project Member

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

Comment 4 by sheriffbot on Tue, Feb 22, 2022, 5:53 PM EST Project Member

Labels: Security_Impact-Extended

Comment 5 by jmad...@chromium.org on Wed, Feb 23, 2022, 7:43 AM EST Project Member

Dana, we don't (at this point) use the Vulkan back-end on Android. Maybe we can reduce this from Critical?

Comment 6 by jmad...@chromium.org on Wed, Feb 23, 2022, 7:44 AM EST Project Member

Labels: -OS-Android

Comment 7 by sheriffbot on Thu, Feb 24, 2022, 12:47 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 8 by sheriffbot on Thu, Feb 24, 2022, 1:13 PM EST Project Member

Labels: -Pri-1 Pri-0

Setting Pri-0 to match security severity Critical. 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 9 by jmad...@chromium.org on Tue, Mar 1, 2022, 1:11 PM EST Project Member

Labels: -Security_Severity-Critical Security_Severity-High Pri-1

Adjusting labels to reflect the sandboxed process. (Not an Android bug).

Comment 10 by jmad...@chromium.org on Tue, Mar 1, 2022, 3:18 PM EST Project Member

Cc: cclao@google.com

Comment 11 by Git Watcher on Mon, Mar 7, 2022, 1:11 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/ea70300ba04404ba0c1cacf2173a0a1e3b443adf

commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 19:55:00 2022

Fix base level changes not updating FBO completeness check.

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Reviewed-by: Charlie Lao <cclao@google.com>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/ea70300ba04404ba0c1cacf2173a0a1e3b443adf/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/ea70300ba04404ba0c1cacf2173a0a1e3b443adf/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/ea70300ba04404ba0c1cacf2173a0a1e3b443adf/src/libANGLE/Texture.cpp
[modify] https://crrev.com/ea70300ba04404ba0c1cacf2173a0a1e3b443adf/src/libANGLE/renderer/vulkan/vk_helpers.cpp
[modify]
https://crrev.com/ea70300ba04404ba0c1cacf2173a0a1e3b443adf/src/tests/capture_replay_tests/capture_replay_expectations.txt

Comment 12 by Git Watcher on Mon, Mar 7, 2022, 5:26 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/04d9d2bb8389539411d6216c1d4ff08d7b84d7a9

commit 04d9d2bb8389539411d6216c1d4ff08d7b84d7a9
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Mon Mar 07 22:25:11 2022

Roll ANGLE from 53eb7671772b to ea70300ba044 (2 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/53eb7671772b..ea70300ba044

2022-03-07 jmadill@chromium.org Fix base level changes not updating FBO completeness check.
2022-03-07 antonio.caggiano@collabora.com EGL: Validate and implement dmabuf extensions

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/angle-chromium-autoroll
Please CC yuxinhu@google.com on the revert to ensure that a human
is aware of the problem.

To file a bug in ANGLE: https://bugs.chromium.org/p/angleproject/issues/entry

To file a bug in ANGLE: https://bugs.chromium.org/p/angleproject/issues/entry
To file a bug in Chromium: https://bugs.chromium.org/p/chromium/issues/entry

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+doc/main/autoroll/README.md

Cq-Include-Trybots:
luci.chromium.try:android_optional_gpu_tests_rel;luci.chromium.try:linux_optional_gpu_tests_rel;luci.chromium.try:mac_optional_gpu_tests_rel;luci.chromium.try:win_optional_gpu_tests_rel;luci.chromium.try:linux-swangle-try-x64;luci.chromium.try:win-swangle-try-x86
~~Bug: chromium:1299264~~
Tbr: yuxinhu@google.com
Change-Id: Iefa5e1aec5e5cd15baead1ce5bea73bfdf43032f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508211
Commit-Queue: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Bot-Commit: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/heads/main@{#978477}

[modify] https://crrev.com/04d9d2bb8389539411d6216c1d4ff08d7b84d7a9/DEPS

Comment 13 by jmad...@chromium.org on Tue, Mar 8, 2022, 9:30 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 14 by sheriffbot on Tue, Mar 8, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 15 by sheriffbot on Tue, Mar 8, 2022, 1:41 PM EST Project Member

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

Comment 16 by sheriffbot on Tue, Mar 8, 2022, 2:02 PM EST Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (978477) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (978477) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (978477) appears to be after beta branch point (972766).

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

Comment 17 by sheriffbot on Tue, Mar 8, 2022, 2:13 PM EST Project Member

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

Merge review required: a commit with DEPS changes was detected.

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 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 18 by sheriffbot on Tue, Mar 8, 2022, 2:13 PM EST Project Member

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

Merge review required: a commit with DEPS changes was detected.

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), ceb (ChromeOS), pbommana (Desktop)

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

Comment 19 by sheriffbot on Tue, Mar 8, 2022, 2:13 PM EST Project Member

Labels: -Merge-Request-98 Merge-Review-98

Merge review required: a commit with DEPS changes was detected.

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), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 20 by jmad...@chromium.org on Tue, Mar 8, 2022, 2:14 PM EST Project Member

1. use-after-free
2. https://chromium-review.googlesource.com/c/angle/angle/+/3498282
3. not yet verified in canary, will be in a couple days
4. no

Comment 21 by amyressler@chromium.org on Wed, Mar 9, 2022, 5:29 PM EST Project Member

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

M100 merge approved, please merge to branch 4896 as it appears the original commit and ANGLE roll landed past M100 branch point

M99 merge approved, please merge this fix to branch 4844 by NLT noon PST tomorrow, Thursday 10 March so this fix can be included in the next stable security refresh

M98 merge approved, please merge to branch 4758 so this fix can be included in stable support -- thank you!

Comment 22 by Git Watcher on Thu, Mar 10, 2022, 9:39 AM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/b0f33007113dc18886673b5ae14ec3964e1d65e7

commit b0f33007113dc18886673b5ae14ec3964e1d65e7
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 19:55:00 2022

[M100] Fix base level changes not updating FBO completeness check.

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Reviewed-by: Charlie Lao <cclao@google.com>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3516965
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/b0f33007113dc18886673b5ae14ec3964e1d65e7/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/b0f33007113dc18886673b5ae14ec3964e1d65e7/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/b0f33007113dc18886673b5ae14ec3964e1d65e7/src/libANGLE/Texture.cpp
[modify] https://crrev.com/b0f33007113dc18886673b5ae14ec3964e1d65e7/src/libANGLE/renderer/vulkan/vk_helpers.cpp
[modify]
https://crrev.com/b0f33007113dc18886673b5ae14ec3964e1d65e7/src/tests/capture_replay_tests/capture_replay_expectations.txt

ions.txt

Comment 23 by sheriffbot on Thu, Mar 10, 2022, 9:39 AM EST 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?
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 24 by Git Watcher on Thu, Mar 10, 2022, 11:33 AM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/8799da6ff6cb5d0655986e83221ffa26d2715a65

commit 8799da6ff6cb5d0655986e83221ffa26d2715a65
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 19:55:00 2022

[M98] Fix base level changes not updating FBO completeness check.

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Reviewed-by: Charlie Lao <cclao@google.com>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3516967
Reviewed-by: Prudhvikumar Bommana <pbommana@google.com>
Reviewed-by: Ian Elliott <ianelliott@google.com>

[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/libANGLE/Texture.cpp
[modify]
https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/tests/capture_replay_tests/capture_replay_expectations.txt

Comment 25 by Git Watcher on Thu, Mar 10, 2022, 11:33 AM EST Project Member

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/0085e8907617077700ffe740111d2d871b7745b8

commit 0085e8907617077700ffe740111d2d871b7745b8
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 19:55:00 2022

[M99] Fix base level changes not updating FBO completeness check.

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Reviewed-by: Charlie Lao <cclao@google.com>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3516966
Reviewed-by: Prudhvikumar Bommana <pbommana@google.com>
Commit-Queue: Prudhvikumar Bommana <pbommana@google.com>
Reviewed-by: Ian Elliott <ianelliott@google.com>

[modify] https://crrev.com/0085e8907617077700ffe740111d2d871b7745b8/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/0085e8907617077700ffe740111d2d871b7745b8/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/0085e8907617077700ffe740111d2d871b7745b8/src/libANGLE/Texture.cpp
[modify] https://crrev.com/0085e8907617077700ffe740111d2d871b7745b8/src/libANGLE/renderer/vulkan/vk_helpers.cpp
[modify]
https://crrev.com/0085e8907617077700ffe740111d2d871b7745b8/src/tests/capture_replay_tests/capture_replay_expectations.txt

Comment 26 by Git Watcher on Thu, Mar 10, 2022, 11:34 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/8799da6ff6cb5d0655986e83221ffa26d2715a65

commit 8799da6ff6cb5d0655986e83221ffa26d2715a65
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 19:55:00 2022

[M98] Fix base level changes not updating FBO completeness check.

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Reviewed-by: Charlie Lao <cclao@google.com>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3516967
Reviewed-by: Prudhvikumar Bommana <pbommana@google.com>
Reviewed-by: Ian Elliott <ianelliott@google.com>

[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/libANGLE/Texture.cpp
[modify]

[modify]
https://crrev.com/8799da6ff6cb5d0655986e83221ffa26d2715a65/src/tests/capture_replay_tests/capture_replay_expectations.txt

Comment 27 by Git Watcher on Thu, Mar 10, 2022, 2:02 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/aa07ecef98d7bb9c149f3bb7f5542d5da914fe79

commit aa07ecef98d7bb9c149f3bb7f5542d5da914fe79
Author: Geoff Lang <geofflang@google.com>
Date: Thu Mar 10 18:53:22 2022

[M98] Fix compile warning about uninitialized fields

The merge of
https://chromium-review.googlesource.com/c/angle/angle/+/3516967
caused compile errors on the release builders because they have
different warnings enabled versus standalone ANGLE.

~~Bug: chromium:1299264~~
Change-Id: I7927dc24b6b8731fbc4a0fde15a7cea9144af416
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3517351
Reviewed-by: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/aa07ecef98d7bb9c149f3bb7f5542d5da914fe79/src/libANGLE/renderer/vulkan/RendererVk.cpp

Comment 28 by Git Watcher on Thu, Mar 10, 2022, 2:15 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/29b222a3c07c541cafa459ae6886134da3493a4b

commit 29b222a3c07c541cafa459ae6886134da3493a4b
Author: Geoff Lang <geofflang@google.com>
Date: Thu Mar 10 18:53:22 2022

[M99] Fix compile warning about uninitialized fields

The merge of
https://chromium-review.googlesource.com/c/angle/angle/+/3516967
caused compile errors on the release builders because they have
different warnings enabled versus standalone ANGLE.

~~Bug: chromium:1299264~~
Change-Id: I7927dc24b6b8731fbc4a0fde15a7cea9144af416
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3517351
Reviewed-by: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit aa07ecef98d7bb9c149f3bb7f5542d5da914fe79)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3517355
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Reviewed-by: Srinivas Sista <srinivassista@chromium.org>

[modify] https://crrev.com/29b222a3c07c541cafa459ae6886134da3493a4b/src/libANGLE/renderer/vulkan/RendererVk.cpp

Comment 29 by rzanoni@google.com on Fri, Mar 11, 2022, 9:19 AM EST Project Member

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

Comment 30 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:25 PM EST Project Member

Labels: Release-1-M99

Comment 31 by rzanoni@google.com on Mon, Mar 14, 2022, 8:42 AM EDT Project Member

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

Comment 32 by sheriffbot on Mon, Mar 14, 2022, 8:47 AM 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 33 by rzanoni@google.com on Mon, Mar 14, 2022, 8:52 AM EDT Project Member

1. Just https://crrev.com/c/3516115
2. Low, only a few conflicts regarding functions that are defined on main and not in M96
3. 98, 99, 100
4. Yes

Comment 34 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0978 CVE_description-missing

Comment 35 by gmpritchard@google.com on Tue, Mar 15, 2022, 9:53 AM EDT Project Member

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

Comment 36 by Git Watcher on Tue, Mar 15, 2022, 10:09 AM EDT Project Member

Labels: merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/2a58cc86bf5a761e170d6e33422fb2e140a0324b

commit 2a58cc86bf5a761e170d6e33422fb2e140a0324b
Author: Jamie Madill <jmadill@chromium.org>

Date: Tue Mar 01 19:55:00 2022

[M96-LTS] Fix base level changes not updating FBO completeness check

[M96-LTS] Fix base level changes not updating FBO completeness check.

M96 merge issues:
 - RendererVk.cpp:
 conflicting kSkippedSyncvalMessages entries
 - vk_helpers.cpp
 getRenderPassWriteCommandCount() not present in M96
 - capture_replay_expectations.txt:
 conflicting skipped test entries
 - src/tests/gl_tests/FramebufferTest.cpp
 RedefineLayerAttachment not present in M96

~~Bug: chromium:1299264~~
Change-Id: I0881a4916c3eeb9ee023d28d207795899417d530
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498282
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Auto-Submit: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit ea70300ba04404ba0c1cacf2173a0a1e3b443adf)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3516115
Reviewed-by: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/2a58cc86bf5a761e170d6e33422fb2e140a0324b/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/2a58cc86bf5a761e170d6e33422fb2e140a0324b/src/libANGLE/renderer/vulkan/RendererVk.cpp
[modify] https://crrev.com/2a58cc86bf5a761e170d6e33422fb2e140a0324b/src/libANGLE/Texture.cpp
[modify] https://crrev.com/2a58cc86bf5a761e170d6e33422fb2e140a0324b/src/libANGLE/renderer/vulkan/vk_helpers.cpp

Comment 37 by rzanoni@google.com on Tue, Mar 15, 2022, 10:20 AM EDT Project Member

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

Comment 38 by amyressler@google.com on Wed, Mar 16, 2022, 9:46 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-7000

*** 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 39 by amyressler@chromium.org on Wed, Mar 16, 2022, 9:54 PM EDT Project Member

Congratulations, Cassidy Kim! The VRP Panel has decided to award you $7,000 for this report. Thank you for your efforts and reporting this issue to us-- nice work!

Comment 40 by amyressler@google.com on Thu, Mar 17, 2022, 5:26 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 41 by sheriffbot on Tue, Jun 14, 2022, 1:27 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 42 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 43 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:18 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing