☆ Starred by 3 users

Owner:	jmad...@chromium.org
CC:	syoussefi@chromium.org backer@chromium.org penghuang@chromium.org vasilyt@chromium.org egdaniel@google.com
Status:	Fixed *(Closed)*
Components:	Internals>GPU>Vulkan
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
M-100
reward-10000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-100
FoundIn-100
Security_Impact-Extended
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1477

Issue 1313905: Security: [ANGLE] Heap use-after-free in ContextVk::onBeginTransformFeedback

Reported by ggabu...@gmail.com on Wed, Apr 6, 2022, 8:54 AM EDT

Code

VULNERABILITY DETAILS

There is a heap uss-after-free vulnerability that is caused by the ContextVk::onBeginTransformFeedback function.
This vulnerability exists in the Vulkan backend.

When glBeginTransformFeedback() is called, the TransformFeedbackVk::begin function calls initializeXFBBuffersDesc.

```
-------------------------------------------------------------------------------------------
void TransformFeedbackVk::initializeXFBBuffersDesc(ContextVk *contextVk, size_t xfbBufferCount)
{
    mXFBBuffersDesc.reset();
    for (size_t bufferIndex = 0; bufferIndex < xfbBufferCount; ++bufferIndex)
    {
        const gl::OffsetBindingPointer<gl::Buffer> &binding = mState.getIndexedBuffer(bufferIndex);
        ASSERT(binding.get());

        BufferVk *bufferVk = vk::GetImpl(binding.get());

        if (bufferVk->isBufferValid())
        {
            mBufferHelpers[bufferIndex] = &bufferVk->getBuffer();
            mBufferOffsets[bufferIndex] =
                binding.getOffset() + mBufferHelpers[bufferIndex]->getOffset();
            mBufferSizes[bufferIndex] = gl::GetBoundBufferAvailableSize(binding);
            mBufferObserverBindings[bufferIndex].bind(bufferVk);
        }
-------------------------------------------------------------------------------------------
```

|mBufferHelpers| has a buffer bound to GL_TRANSFORM_FEEDBACK_BUFFER. This buffer can be freed by glDeleteBuffer().
And in the glResumeTransformFeedback() function, the ContextVk::onBeginTransformFeedback function is called with the |mBufferHelpers| argument.

```
-------------------------------------------------------------------------------------------
angle::Result TransformFeedbackVk::resume(const gl::Context *context)
{
    ....

    return contextVk->onBeginTransformFeedback(xfbBufferCount, mBufferHelpers,
                                               mCounterBufferHelpers);
}
-------------------------------------------------------------------------------------------
```

And in onBeginTransformFeedback, it uses the already freed buffer without any validation.

```
-------------------------------------------------------------------------------------------
angle::Result ContextVk::onBeginTransformFeedback(
    size_t bufferCount
    size_t bufferCount,
    const gl::TransformFeedbackBuffersArray<vk::BufferHelper *> &buffers,
    const gl::TransformFeedbackBuffersArray<vk::BufferHelper> &counterBuffers)
{
    onTransformFeedbackStateChanged();

    bool shouldEndRenderPass = false;

    // If any of the buffers were previously used in the render pass, break the render pass as a
    // barrier is needed.
    for (size_t bufferIndex = 0; bufferIndex < bufferCount; ++bufferIndex)
    {
        const vk::BufferHelper *buffer = buffers[bufferIndex];                  <--- can be freed
        if (mRenderPassCommands->usesBuffer(*buffer))
        {
            shouldEndRenderPass = true;
            break;
        }
    }
--------------------------------------------------------------------------------------
```

This vulnerability causes a simple crash in Swiftshader.

```
--------------------------------------------------------------------------------------
angle::Result TransformFeedbackVk::resume(const gl::Context *context)
{
    ContextVk *contextVk                   = vk::GetImpl(context);
    const gl::ProgramExecutable *executable = contextVk->getState().getProgramExecutable();
    ASSERT(executable);
    size_t xfbBufferCount = executable->getTransformFeedbackBufferCount();

    if (contextVk->getFeatures().emulateTransformFeedback.enabled)
    {
        initializeXFBBuffersDesc(contextVk, xfbBufferCount);
    }

    return contextVk->onBeginTransformFeedback(xfbBufferCount, mBufferHelpers,
                                               mCounterBufferHelpers);
}
--------------------------------------------------------------------------------------
```

On platforms without VK_EXT_transform_feedback(including Swiftshader), emulateTransformFeedback.enabled is true. Therefore, the initializeXFBBuffersDesc function is called.

```
--------------------------------------------------------------------------------------
void TransformFeedbackVk::initializeXFBBuffersDesc(ContextVk *contextVk, size_t xfbBufferCount)
{

    mXFBBuffersDesc.reset();
    for (size_t bufferIndex = 0; bufferIndex < xfbBufferCount; ++bufferIndex)
    {
```

```
    {
        const gl::OffsetBindingPointer<gl::Buffer> &binding = mState.getIndexedBuffer(bufferIndex);
        ASSERT(binding.get());

        BufferVk *bufferVk = vk::GetImpl(binding.get());
---------------------------------------------------------------------------------------
```

However, buffer has already been detached. So the GetImpl function crashes.
If ASSERT is enabled(is_debug = true), Chrome will output an Assert failed error message.

VERSION
Chrome Version: master (and tested on 100.0.4896.75 (Official Build) (64-bit) Stable)
Operating System: Linux (vulkan)

REPRODUCTION CASE
Run the attached poc.html on Vulkan backend (--use-angle=vulkan) (not swiftshader)

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

```
=================================================================
==6788==ERROR: AddressSanitizer: heap-use-after-free on address 0x1205380bf774 at pc 0x7ffa987bc62f bp
0x00ac4fdfe340 sp 0x00ac4fdfe388
READ of size 4 at 0x1205380bf774 thread T0
==6788==WARNING: Failed to use and restart external symbolizer!
==6788==*** WARNING: Failed to initialize DbgHelp!              ***
==6788==*** Most likely this means that the app is already      ***
==6788==*** using DbgHelp, possibly with incompatible flags.    ***
==6788==*** Due to technical reasons, symbolization might crash ***
==6788==*** or produce wrong results.                           ***
    #0 0x7ffa987bc62e in rx::vk::CommandBufferHelperCommon::usesBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:1330
    #1 0x7ffa9866fc24 in rx::ContextVk::onBeginTransformFeedback
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:5096
    #2 0x7ffa980d2239 in gl::TransformFeedback::resume
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\TransformFeedback.cpp:197
    #3 0x7ffa97f8bfb1 in gl::Context::resumeTransformFeedback
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:7839
    #4 0x7ffa97ef42d8 in GL_ResumeTransformFeedback
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_3_0_autogen.cpp:2127

    #5 0x7ffaafbc3f96 in gpu::gles2::GLES2DecoderPassthroughImpl::DoResumeTransformFeedback
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:2581
    #6 0x7ffaabf697fb in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
```

```
   #6 0x7ffaabf697fb in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:870
   #7 0x7ffaabf68c50 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:808
   #8 0x7ffaa8d6804b in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
   #9 0x7ffaa609af6c in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:500
   #10 0x7ffaa609a146 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:152
   #11 0x7ffaa60a6b37 in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:670
   #12 0x7ffaa60b199f in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
   #13 0x7ffaa5cdfc6c in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:691
   #14 0x7ffaa4820714 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
   #15 0x7ffaa76c3215 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:386
   #16 0x7ffaa76c2809 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:291
   #17 0x7ffaa769f8aa in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
   #18 0x7ffaa76c4980 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:498
   #19 0x7ffaa479b2b3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
   #20 0x7ffaa6fce29e in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:405
   #21 0x7ffaa43ca48b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:682
   #22 0x7ffaa43cc0c7 in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1021
   #23 0x7ffaa43c8abb in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:407
   #24 0x7ffaa43c9244 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:435
   #25 0x7ffa992514ca in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176
   #26 0x7ff7b0595b16 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:167
   #27 0x7ff7b0592b5f in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
   #28 0x7ff7b098f87b in __scrt_common_main_seh
d:\a01\_work\12\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
   #29 0x7ffb54ed7033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
   #30 0x7ffb55c22650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x1205380bf774 is located 180 bytes inside of 312-byte region [0x1205380bf6c0,0x1205380bf7f8)
freed by thread T0 here:
   #0 0x7ff7b063e8cb in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
   #1 0x7ffa98628c89 in rx::BufferVk::~BufferVk
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\BufferVk.cpp:238
   #2 0x7ffa97f304e2 in gl::Buffer::~Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:55
   #3 0x7ffa97f31ec3 in gl::Buffer::~Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:54
   #4 0x7ffa98089833 in gl::TypedResourceManager<gl::Sampler,gl::SamplerManager,gl::SamplerID>::deleteObject

C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:96
   #5 0x7ffa97f844bd in gl::Context::deleteBuffers
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:6786
```

```
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:6786
    #6 0x7ffa97ee0897 in GL_DeleteBuffers
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:819
    #7 0x7ffaafbb2d85 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDeleteBuffers
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:1012
    #8 0x7ffaabf697fb in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:870
    #9 0x7ffaabf68c50 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:808
    #10 0x7ffaa8d6804b in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #11 0x7ffaa609af6c in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:500
    #12 0x7ffaa609a146 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:152
    #13 0x7ffaa60a6b37 in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:670
    #14 0x7ffaa60b199f in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
    #15 0x7ffaa5cdfc6c in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:691
    #16 0x7ffaa4820714 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
    #17 0x7ffaa76c3215 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:386
    #18 0x7ffaa76c2809 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:291
    #19 0x7ffaa769f8aa in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
    #20 0x7ffaa76c4980 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:498
    #21 0x7ffaa479b2b3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
    #22 0x7ffaa6fce29e in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:405
    #23 0x7ffaa43ca48b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:682
    #24 0x7ffaa43cc0c7 in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1021
    #25 0x7ffaa43c8abb in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:407
    #26 0x7ffaa43c9244 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:435
    #27 0x7ffa992514ca in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176

previously allocated by thread T0 here:
    #0 0x7ff7b063e9cb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffa98beefc6 in operator new d:\a01\_work\12\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffa9866d8c9 in rx::ContextVk::createBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:4814
    #3 0x7ffa97f3024a in gl::Buffer::Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:47
    #4 0x7ffa9808b1a3 in gl::BufferManager::AllocateNewObject
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:114
    #5 0x7ffa97eebc17 in gl::TypedResourceManager<gl::Buffer,gl::BufferManager,gl::BufferID>::checkObjectAllocationImpl<>

C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.h:117
    #6 0x7ffa97edda65 in GL_BindBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:118
```

```
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:118
   #7 0x7ffaafbadac7 in gpu::gles2::GLES2DecoderPassthroughImpl::DoBindBuffer
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:390
   #8 0x7ffaabf697fb in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:870
   #9 0x7ffaabf68c50 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:808
   #10 0x7ffaa8d6804b in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
   #11 0x7ffaa609af6c in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:500
   #12 0x7ffaa609a146 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:152
   #13 0x7ffaa60a6b37 in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:670
   #14 0x7ffaa60b199f in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
   #15 0x7ffaa5cdfc6c in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:691
   #16 0x7ffaa4820714 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
   #17 0x7ffaa76c3215 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:386
   #18 0x7ffaa76c2809 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:291
   #19 0x7ffaa769f8aa in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
   #20 0x7ffaa76c4980 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:498
   #21 0x7ffaa479b2b3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
   #22 0x7ffaa6fce29e in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:405
   #23 0x7ffaa43ca48b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:682
   #24 0x7ffaa43cc0c7 in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1021
   #25 0x7ffaa43c8abb in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:407
   #26 0x7ffaa43c9244 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:435
   #27 0x7ffa992514ca in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176

SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:1330 in
rx::vk::CommandBufferHelperCommon::usesBuffer
Shadow bytes around the buggy address:
  0x0421def17e90: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x0421def17ea0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0421def17eb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0421def17ec0: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x0421def17ed0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x0421def17ee0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]fd
  0x0421def17ef0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa

  0x0421def17f00: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0421def17f10: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0421def17f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0421def17f20: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0421def17f30: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==6788==ABORTING
[20576:20036:0406/204207.698:ERROR:gpu_process_host.cc(973)] GPU process exited unexpectedly: exit_code=1
```

CREDIT INFORMATION
Reporter credit: SeongHwan Park (SeHwa)

poc.html
1.7 KB View Download

Comment 1 by sheriffbot on Wed, Apr 6, 2022, 8:56 AM EDT Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Wed, Apr 6, 2022, 5:26 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=6205249010073600.

Comment 3 by rsesek@chromium.org on Wed, Apr 6, 2022, 5:27 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: jmad...@chromium.org
Cc: syoussefi@chromium.org
Labels: FoundIn-100 Security_Impact-Stable Security_Severity-High OS-Linux OS-Windows Pri-1
Components: Internals>GPU>Vulkan

Thanks, I can reproduce this on Linux.

Comment 4 by sheriffbot on Wed, Apr 6, 2022, 5:29 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 5 by ClusterFuzz on Wed, Apr 6, 2022, 9:57 PM EDT Project Member

Labels: OS-Android

Comment 6 by sheriffbot on Thu, Apr 7, 2022, 12:47 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 7 by jmad...@chromium.org on Thu, Apr 7, 2022, 2:14 PM EDT Project Member

Labels: -OS-Android OS-Mac

Won't affect Android, may affect Mac.

Comment 8 by jmad...@chromium.org on Mon, Apr 11, 2022, 11:41 AM EDT Project Member

Status: Duplicate (was: Assigned)
Mergedinto: 1305190

Believe this is a duplicate of an earlier report, fixed in 101.

Comment 9 by jmad...@chromium.org on Mon, Apr 11, 2022, 11:43 AM EDT Project Member

Status: Assigned (was: Duplicate)

Seems to still repro in ToT, looking again.

Comment 10 by ggabu...@gmail.com on Mon, Apr 11, 2022, 9:21 PM EDT

I just looked at https://crrev.com/c/3578378/
May I know why is this commit's bug number 1305190?
The test code included in the patch seems to be the PoC I uploaded.

I don't know exactly because I can't see the 1305190 report,
but 1305190 seems to have been patched in commit 708ce9cfd63.
My PoC is still valid with this patch applied.

Thanks.

Comment 11 by jmad...@chromium.org on Tue, Apr 12, 2022, 10:53 AM EDT Project Member

Status: Fixed (was: Assigned)

Ah, I used the wrong bug ID. This bug was fixed by

commit 5c85fd4e11a3835a0719223a7cedb978d309da21
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 11 16:29:00 2022

Add error check on resuming XFB with deleted buffer.

~~Bug: chromium:1305190~~
Change-Id: I22c6f6400b05ca32c922fba9a3b9d4b5841ca8b8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378

Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>

Comment 12 by sheriffbot on Tue, Apr 12, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 13 by sheriffbot on Tue, Apr 12, 2022, 1:40 PM EDT Project Member

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

Comment 14 by sheriffbot on Tue, Apr 12, 2022, 2:01 PM EDT Project Member

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

This is sufficiently serious that it should be merged to stable. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M100. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M101. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

Comment 15 by sheriffbot on Tue, Apr 12, 2022, 2:04 PM EDT Project Member

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

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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 16 by sheriffbot on Tue, Apr 12, 2022, 2:04 PM EDT Project Member

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

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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 17 by amyressler@chromium.org on Fri, Apr 15, 2022, 8:47 PM EDT Project Member

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

M101 and M100 merges approved; please merge this fix to branches 4951 and 4896 respectively and before 10am PDT Tuesday, 19 April so this fix can be included in the M101 Stable cut and M100 Extended -- thanks!

Comment 18 by Git Watcher on Tue, Apr 19, 2022, 9:50 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/e37380e62a427cbb7172b6c17f8752ab96abf356

commit e37380e62a427cbb7172b6c17f8752ab96abf356
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 11 16:29:00 2022

[M101] Add error check on resuming XFB with deleted buffer.

~~Bug: chromium:1313905~~
Change-Id: I22c6f6400b05ca32c922fba9a3b9d4b5841ca8b8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 5c85fd4e11a3835a0719223a7cedb978d309da21)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3594102
Reviewed-by: Shahbaz Youssefi <syoussefi@chromium.org>

[modify] https://crrev.com/e37380e62a427cbb7172b6c17f8752ab96abf356/src/libANGLE/validationES3.cpp

Comment 19 by Git Watcher on Tue, Apr 19, 2022, 9:50 AM EDT 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/+/d49484c21e3c43b06dbe1274e94908559dc444a1

commit d49484c21e3c43b06dbe1274e94908559dc444a1
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 11 16:29:00 2022

[M100] Add error check on resuming XFB with deleted buffer.

~~Bug: chromium:1313905~~
Change-Id: I22c6f6400b05ca32c922fba9a3b9d4b5841ca8b8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 5c85fd4e11a3835a0719223a7cedb978d309da21)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3594103
Reviewed-by: Shahbaz Youssefi <syoussefi@chromium.org>

[modify] https://crrev.com/d49484c21e3c43b06dbe1274e94908559dc444a1/src/libANGLE/validationES3.cpp

Comment 20 by Git Watcher on Tue, Apr 19, 2022, 9:51 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/e37380e62a427cbb7172b6c17f8752ab96abf356

commit e37380e62a427cbb7172b6c17f8752ab96abf356
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 11 16:29:00 2022

[M101] Add error check on resuming XFB with deleted buffer.

~~Bug: chromium:1313905~~
Change-Id: I22c6f6400b05ca32c922fba9a3b9d4b5841ca8b8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 5c85fd4e11a3835a0719223a7cedb978d309da21)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3594102
Reviewed-by: Shahbaz Youssefi <syoussefi@chromium.org>

[modify] https://crrev.com/e37380e62a427cbb7172b6c17f8752ab96abf356/src/libANGLE/validationES3.cpp

Comment 21 by amyressler@google.com on Thu, Apr 21, 2022, 8:40 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-10000

*** 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

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 by amyressler@chromium.org on Thu, Apr 21, 2022, 9:29 PM EDT Project Member

Congratulations, SeongHwan! The VRP Panel has decided to award you $10,000 for this report. Thank you for your efforts and excellent work in reporting GPU process memory corruption bugs!

Comment 23 by amyressler@chromium.org on Mon, Apr 25, 2022, 12:47 PM EDT Project Member

Labels: Release-0-M101

Comment 24 by amyressler@google.com on Mon, Apr 25, 2022, 4:12 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@google.com on Tue, Apr 26, 2022, 4:30 PM EDT Project Member

Labels: CVE-2022-1477 CVE_description-missing

Comment 26 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 27 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 28 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing