bugs chromium ▾ New issue Open issues ▾ Search chromium issue ▾ Sign in

☆ Starred by 6 users

Owner:	cclao@google.com **Last visit > 30 days ago**
CC:	rzanoni@google.com nicol...@google.com sugoi@chromium.org capn@chromium.org cclao@google.com srinivassista@google.com abdolrashidi@google.com amyressler@chromium.org jmad...@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>GPU>ANGLE Internals>GPU>SwiftShader
Modified:	Jul 29, 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
CVE_description-submitted
external_security_report
M-99
reward-7000
Target-99
FoundIn-98
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100

Release-0-M101
CVE-2022-1478

Issue 1299261: Security: [ANGLE] Heap overflow read in vk::IndexBuffer::getIndexBuffers

Reported by ggabu...@gmail.com on Sun, Feb 20, 2022, 9:03 AM EST

Code

VULNERABILITY DETAILS

There is a heap use-after-free vulnerability that could be triggered in Swiftshader.
It seems that this vulnerability started in commit 8589c456a2fb1a4041a6935f0524a0fb74ddcd64.

VERSION

Chrome Version: master (956307 ~ latest), (99.0.4844.35 (Official Build) (64-bit) beta)
Operating System: Windows 10 x64

REPRODUCTION CASE

Run the attached poc.html (with --disable-gpu)

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: GPU Process
Crash State:

```
=================================================================
==760==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x1299f01d1826 at pc 0x7fff81a40c00 bp
0x001a275ff320 sp 0x001a275ff368
READ of size 2 at 0x1299f01d1826 thread T5
==760==WARNING: Failed to use and restart external symbolizer!
==760==*** WARNING: Failed to initialize DbgHelp!              ***
==760==*** Most likely this means that the app is already      ***
==760==*** using DbgHelp, possibly with incompatible flags.    ***
==760==*** Due to technical reasons, symbolization might crash ***
==760==*** or produce wrong results.                           ***
    #0 0x7fff81a40bff in vk::IndexBuffer::getIndexBuffers
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Device\Context.cpp:113
    #1 0x7fff8197de42 in vk::GraphicsPipeline::getIndexBuffers
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkPipeline.cpp:289
    #2 0x7fff81940977 in `anonymous namespace'::CmdDrawBase::draw
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkCommandBuffer.cpp:788
    #3 0x7fff81940ebd in `anonymous namespace'::CmdDrawIndexed::execute

C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkCommandBuffer.cpp:853
    #4 0x7fff8193bd1b in vk::CommandBuffer::submit
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkCommandBuffer.cpp:2117
```

```
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkCommandBuffer.cpp:2117
    #5 0x7fff8198b709 in vk::Queue::submitQueue
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkQueue.cpp:104
    #6 0x7fff8198a429 in vk::Queue::taskLoop
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkQueue.cpp:156
    #7 0x7fff8198d223 in
std::__1::__thread_proxy<std::__1::tuple<std::__1::unique_ptr<std::__1::__thread_struct,std::__1::default_delete<std::__1::_
_thread_struct> >,void (vk::Queue::*)(marl::Scheduler *),vk::Queue *,marl::Scheduler *> >
C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\thread:291
    #8 0x7fff82305087 in thread_start<unsigned int (__cdecl*)(void *),1>
C:\b\s\w\ir\cache\builder\src\out\Release_x64\minkernel\crts\ucrt\src\appcrt\startup\thread.cpp:97
    #9 0x7ff7de167ba3 in __asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_thread.cpp:277
    #10 0x7fffb8117033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #11 0x7fffb9fa2650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x1299f01d1827 is located 0 bytes to the right of 8388647-byte region [0x1299ef9d1800,0x1299f01d1827)
allocated by thread T0 here:
    #0 0x7ff7de15d2cb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7fff81cdda66 in sw::allocateZeroOrPoison
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\System\Memory.cpp:116
    #2 0x7fff81957b50 in vk::DeviceMemory::allocateBuffer
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkDeviceMemory.cpp:323
    #3 0x7fff81956dfd in vk::DeviceMemory::Allocate
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkDeviceMemory.cpp:103
    #4 0x7fff819a5378 in vkAllocateMemory
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\libVulkan.cpp:1124
    #5 0x7fff4e3d811d in rx::`anonymous namespace'::FindAndAllocateCompatibleMemory
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_utils.cpp:103
    #6 0x7fff4e3d4ab5 in rx::`anonymous namespace'::AllocateAndBindBufferOrImageMemory<rx::vk::Buffer>
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_utils.cpp:181
    #7 0x7fff4e3d4009 in rx::vk::AllocateBufferMemory
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_utils.cpp:600
    #8 0x7fff4e388176 in rx::vk::BufferPool::allocateNewBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:2693
    #9 0x7fff4e388f82 in rx::vk::BufferPool::allocateBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:2742
    #10 0x7fff4e39499a in rx::vk::BufferHelper::initSuballocation
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:3938
    #11 0x7fff4e394c87 in rx::vk::BufferHelper::allocateForCopyImage
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:4017
    #12 0x7fff4e3a859a in rx::vk::ImageHelper::stageSubresourceUpdateImpl
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:6152
    #13 0x7fff4e3ac402 in rx::vk::ImageHelper::stageSubresourceUpdate
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:6526
    #14 0x7fff4e2f4f20 in rx::TextureVk::setSubImageImpl
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\TextureVk.cpp:554
    #15 0x7fff4e2f4206 in rx::TextureVk::setImageImpl
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\TextureVk.cpp:406
    #16 0x7fff4e2f3f28 in rx::TextureVk::setImage
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\TextureVk.cpp:324

    #17 0x7fff4dca2811 in gl::Texture::setImage C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Texture.cpp:1240
    #18 0x7fff4db576e9 in gl::Context::texImage3D
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:4993
```

```
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:4993
   #19 0x7fff4db577f5 in gl::Context::texImage3DRobust
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:5010
   #20 0x7fff4dae7aa5 in GL_TexImage3DRobustANGLE
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_ext_autogen.cpp:1819
   #21 0x7fff5dbd548e in gl::GLApiBase::glTexImage3DRobustANGLEFn
C:\b\s\w\ir\cache\builder\src\ui\gl\gl_bindings_autogen_gl.cc:5901
   #22 0x7fff650948ac in gpu::gles2::GLES2DecoderPassthroughImpl::DoTexImage3D
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:2757
   #23 0x7fff650ce5f4 in gpu::gles2::GLES2DecoderPassthroughImpl::HandleTexImage3D
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_handlers.cc:1229
   #24 0x7fff61510361 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:871
   #25 0x7fff6150f7a8 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:809
   #26 0x7fff5e3785da in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
   #27 0x7fff5b797df4 in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:499

Thread T5 created by T0 here:
   #0 0x7ff7de168632 in __asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_win.cpp:146
   #1 0x7fff82304f62 in _beginthreadex
C:\b\s\w\ir\cache\builder\src\out\Release_x64\minkernel\crts\ucrt\src\appcrt\startup\thread.cpp:209
   #2 0x7fff81f15703 in std::__1::__libcpp_thread_create
C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\src\support\win32\thread_win32.cpp:207
   #3 0x7fff8198a735 in std::__1::thread::thread<void (vk::Queue::*)(marl::Scheduler *),vk::Queue *,marl::Scheduler *&,void>
C:\b\s\w\ir\cache\builder\src\buildtools\third_party\libc++\trunk\include\thread:307
   #4 0x7fff8198a16b in vk::Queue::Queue C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkQueue.cpp:38
   #5 0x7fff8194c2ea in vk::Device::Device C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkDevice.cpp:138
   #6 0x7fff819a2c2b in vk::DispatchableObject<vk::Device,VkDevice_T *>::Create<VkDeviceCreateInfo,vk::PhysicalDevice
*,const VkPhysicalDeviceFeatures *,std::__1::shared_ptr<marl::Scheduler> >
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\VkObject.hpp:147
   #7 0x7fff819a2532 in vkCreateDevice C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Vulkan\libVulkan.cpp:1006
   #8 0x7fff85b5fbf4 in terminator_CreateDevice C:\b\s\w\ir\cache\builder\src\third_party\vulkan-deps\vulkan-
loader\src\loader\loader.c:6009
   #9 0x7fff85b59f4f in loader_create_device_chain C:\b\s\w\ir\cache\builder\src\third_party\vulkan-deps\vulkan-
loader\src\loader\loader.c:5248
   #10 0x7fff85b58a32 in loader_layer_create_device C:\b\s\w\ir\cache\builder\src\third_party\vulkan-deps\vulkan-
loader\src\loader\loader.c:4700
   #11 0x7fff85b6e48a in vkCreateDevice C:\b\s\w\ir\cache\builder\src\third_party\vulkan-deps\vulkan-
loader\src\loader\trampoline.c:887
   #12 0x7fff4e2b43dc in rx::RendererVk::initializeDevice
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\RendererVk.cpp:2432
   #13 0x7fff4e2acd19 in rx::RendererVk::initialize
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\RendererVk.cpp:1571
   #14 0x7fff4e24f04b in rx::DisplayVk::initialize
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\DisplayVk.cpp:46
   #15 0x7fff4e3d8975 in rx::DisplayVkWin32::initialize
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\win32\DisplayVkWin32.cpp:62

   #16 0x7fff4db97d51 in egl::Display::initialize C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Display.cpp:962
   #17 0x7fff4daa143c in egl::Initialize C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\egl_stubs.cpp:448
   #18 0x7fff4daa90b8 in EGL_Initialize
   #18 0x7fff4daa90b8 in EGL_Initialize
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_egl_autogen.cpp:330
   #19 0x7fff5b1acaec in gl::GLSurfaceEGL::InitializeDisplay C:\b\s\w\ir\cache\builder\src\ui\gl\gl_surface_egl.cc:1427
   #20 0x7fff5b1a9d66 in gl::GLSurfaceEGL::InitializeOneOff C:\b\s\w\ir\cache\builder\src\ui\gl\gl_surface_egl.cc:988
   #21 0x7fff5dcbcc25 in gl::init::InitializeGLOneOffPlatform C:\b\s\w\ir\cache\builder\src\ui\gl\init\gl_initializer_win.cc:141
   #22 0x7fff5b1e629d in gl::init::InitializeGLOneOffPlatformImplementation
C:\b\s\w\ir\cache\builder\src\ui\gl\init\gl_factory.cc:220
   #23 0x7fff5b1e5b18 in gl::init::`anonymous namespace'::InitializeGLOneOffPlatformHelper
C:\b\s\w\ir\cache\builder\src\ui\gl\init\gl_factory.cc:149
   #24 0x7fff5b1e5e37 in gl::init::InitializeGLNoExtensionsOneOff C:\b\s\w\ir\cache\builder\src\ui\gl\init\gl_factory.cc:176
   #25 0x7fff5b7c557d in gpu::GpuInit::InitializeAndStartSandbox C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_init.cc:405
   #26 0x7fff5c70def4 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:324
   #27 0x7fff559086b7 in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:684
   #28 0x7fff5590a3db in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1044
   #29 0x7fff55906ceb in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:401
   #30 0x7fff5590746f in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:429
   #31 0x7fff4edf14ca in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176
   #32 0x7ff7de0b5b16 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:167
   #33 0x7ff7de0b2b5f in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
   #34 0x7ff7de4ad9a3 in __scrt_common_main_seh
d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
   #35 0x7fffb8117033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
   #36 0x7fffb9fa2650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

SUMMARY: AddressSanitizer: heap-buffer-overflow
C:\b\s\w\ir\cache\builder\src\third_party\swiftshader\src\Device\Context.cpp:113 in vk::IndexBuffer::getIndexBuffers
Shadow bytes around the buggy address:
  0x046d1453a2b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x046d1453a2c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x046d1453a2d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x046d1453a2e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x046d1453a2f0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x046d1453a300: 00 00 00 00[07]fa fa fa fa fa fa fa fa fa fa fa
  0x046d1453a310: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x046d1453a320: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x046d1453a330: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x046d1453a340: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x046d1453a350: 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
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
==760==ABORTING
[9564:10960:0220/224836.408:ERROR:gpu_process_host.cc(974)] GPU process exited unexpectedly: exit_code=1
```

CREDIT INFORMATION
Reporter credit: SeongHwan Park (SeHwa)

poc.html
2.5 KB View Download

Comment 1 by sheriffbot on Sun, Feb 20, 2022, 9:05 AM EST Project Member

Labels: external_security_report

Comment 2 by ggabu...@gmail.com on Sun, Feb 20, 2022, 9:07 AM EST

Sorry. I wrote the title and description wrong. This is a heap buffer overflow(not use-after-free).

Comment 3 by danakj@chromium.org on Tue, Feb 22, 2022, 5:35 PM EST Project Member

Summary: Security: [ANGLE] Heap overflow read in vk::IndexBuffer::getIndexBuffers (was: Security: [ANGLE] Heap use-after-free in vk::IndexBuffer::getIndexBuffers)
Components: Internals>GPU>SwiftShader Internals>GPU>ANGLE

Comment 4 by danakj@chromium.org on Tue, Feb 22, 2022, 5:40 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: sugoi@chromium.org
Cc: jmad...@chromium.org
Labels: FoundIn-99

I can repro in asan build.

Comment 5 by danakj@chromium.org on Tue, Feb 22, 2022, 5:41 PM EST Project Member

Labels: Security_Severity-Critical OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros

Gpu process is unsandboxed in Android, so Critical

Comment 6 by sheriffbot on Tue, Feb 22, 2022, 5:41 PM EST Project Member

Labels: Security_Impact-Beta

Comment 7 by jmad...@chromium.org on Wed, Feb 23, 2022, 8:18 AM EST Project Member

Labels: -OS-Android

We don't use SwiftShader on Android FYI Dana.

Comment 8 by sugoi@chromium.org on Wed, Feb 23, 2022, 9:57 AM EST Project Member

Cc: capn@chromium.org

Comment 9 by sheriffbot on Thu, Feb 24, 2022, 12:47 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 10 by sheriffbot on Thu, Feb 24, 2022, 1:02 PM EST Project Member

Labels: ReleaseBlock-Beta

This is a critical security issue. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 11 by sheriffbot on Thu, Feb 24, 2022, 1:13 PM EST Project Member

Labels: -Pri-3 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 12 by amyressler@chromium.org on Fri, Feb 25, 2022, 1:05 PM EST Project Member

Labels: -Security_Severity-Critical Security_Severity-High

Shifting to high severity for memory corruption in GPU process in SwiftShader which does not impact Android

Comment 13 by jmad...@chromium.org on Fri, Feb 25, 2022, 2:30 PM EST Project Member

Labels: -ReleaseBlock-Beta ReleaseBlock-Stable Pri-1

Comment 14 by jmad...@chromium.org on Fri, Feb 25, 2022, 2:30 PM EST Project Member

Owner: jmad...@chromium.org

Taking as Alexis is heading out for vacation.

Comment 15 by danakj@chromium.org on Fri, Feb 25, 2022, 2:42 PM EST Project Member

> Shifting to high severity for memory corruption in GPU process in SwiftShader which does not impact Android

Thanks, I have trouble telling when a given bug is software renderering only.

Comment 16 by sugoi@chromium.org on Fri, Feb 25, 2022, 3:54 PM EST Project Member

I created an ANGLE end to end test for this:
https://chromium-review.googlesource.com/c/angle/angle/+/3488724
It throws Vulkan Validation Layer errors (VUID-vkCmdDrawIndexed-firstIndex-04932), so that should make it easy to

It throws Vulkan Validation Layer errors (VUID-vkCmdDrawIndexed-firstIndex-04932), so that should make it easy to debug.

Comment 17 by capn@chromium.org on Sat, Feb 26, 2022, 7:56 AM EST Project Member

Cc: -capn@chromium.org nicol...@google.com cclao@google.com

Comment 18 by amyressler@chromium.org on Mon, Feb 28, 2022, 3:35 PM EST Project Member

Labels: -ReleaseBlock-Stable

not a release blocker for M99 stable release tomorrow; removing RBS as was labeled as a M99 release blocker upon initial triage of this as a Critical severity bug

Comment 19 by sheriffbot on Tue, Mar 1, 2022, 12:57 PM EST Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 20 by jmad...@chromium.org on Tue, Mar 1, 2022, 12:59 PM EST Project Member

Cc: abdolrashidi@google.com

Comment 21 by sheriffbot on Tue, Mar 1, 2022, 3:08 PM EST Project Member

Labels: -Security_Impact-Beta Security_Impact-Stable

Comment 22 by sugoi@chromium.org on Tue, Mar 8, 2022, 9:05 AM EST Project Member

Cc: sugoi@chromium.org capn@chromium.org

~~Issue 1303399~~ has been merged into this issue.

Comment 23 by jmad...@chromium.org on Wed, Mar 9, 2022, 11:13 AM EST Project Member

Owner: abdolrashidi@google.com

Comment 24 by sheriffbot on Wed, Mar 9, 2022, 12:21 PM EST Project Member

abdolrashidi: Uh oh! This issue still open and hasn't been updated in the last 17 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 25 by abdolrashidi@google.com on Wed, Mar 9, 2022, 6:02 PM EST Project Member

The VVL error is triggered when comparing the end offset for the draw calls with the allocated size to make sure it has not exceeded the size. Using the end2end test from before (https://chromium-review.googlesource.com/c/angle/angle/+/3488724), it is seen that the offset in the line loop buffer allocation is also present in its subsequent draw calls during the said check. This number seems related to the size in glTexImage3D buffer allocation.

Comment 26 by cclao@google.com on Wed, Mar 9, 2022, 7:52 PM EST Project Member

he problem is that line loop code will convert allocate its own element buffer. When we switch out of line loop mode, we are not resetting the mCurrentElementArrayBuffer which causing draw points uses the wrong element buffer.

Comment 27 by cclao@google.com on Wed, Mar 9, 2022, 8:43 PM EST Project Member

Switch from glDrawElements(GL_UNSIGNED_BYTE) to glDrawElements(GL_UNSIGNED_SHORT) with the same element buffer (i.e, put both uint8_t and uint16_t data in the same buffer) has the exact same bug as well.

Comment 28 by jmad...@chromium.org on Thu, Mar 10, 2022, 9:53 AM EST Project Member

Ah, thanks for identifying the issue Charlie. Seems we need an additional check here. We have this code in setupDraw:

```
  if (mode != mCurrentDrawMode)
  {
     invalidateCurrentGraphicsPipeline();
     mCurrentDrawMode = mode;
     mGraphicsPipelineDesc->updateTopology(&mGraphicsPipelineTransition, mCurrentDrawMode);
  }
```

We could use something similar in setupIndexedDraw.

Comment 29 by amyressler@chromium.org on Thu, Mar 10, 2022, 12:41 PM EST Project Member

Labels: -Security_Impact-Stable -FoundIn-99 FoundIn-98

bad bot -- see comment #18, but also foundin-98

Comment 30 by sheriffbot on Thu, Mar 10, 2022, 12:41 PM EST Project Member

Labels: Security_Impact-Extended

Comment 31 by Git Watcher on Thu, Mar 10, 2022, 5:43 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/b97aab3f862af467de71f8b20f87d3e0ccfe47ad

commit b97aab3f862af467de71f8b20f87d3e0ccfe47ad
Author: Charlie Lao <cclao@google.com>
Date: Thu Mar 10 01:36:24 2022

Vulkan: resync mCurrentElementArrayBuffer when out of lineloop

When glDrawElements is called with GL_UNSIGNED_BYTE type or LineLoop

mode, we will internally allocate an element buffer and copy data to it.
But when we switch out of that mode, we must re-sync
mCurrentElementArrayBuffer to what it should be based on VertexArray.

mCurrentElementArrayBuffer to what it should be based on VertexArray
buffer binding. This CL fix the bug that we were previously not updating
it and end up using the wrong element buffer.

Also added three tests:

DrawWithSameBufferButDifferentTypes: that uses GL_UNSIGNED_BYTE data and
GL_UNSIGNED_SHORT data in the same buffer and switch between these two
data types without incurring buffer change.

DrawWithSameBufferButDifferentModes: draw line mode followed by triangle
without the same element buffer.

DrawArraysLineLoopFollowedByDrawElementsTriangle: draw line mode with
glDrawArrays and then followed by DrawElements.

~~Bug: chromium:1299261~~
Change-Id: I5c471117d300e9fac9127a9d8fa66d48ac312f03
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3513553
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Charlie Lao <cclao@google.com>

[modify] https://crrev.com/b97aab3f862af467de71f8b20f87d3e0ccfe47ad/src/libANGLE/renderer/vulkan/VertexArrayVk.h
[modify] https://crrev.com/b97aab3f862af467de71f8b20f87d3e0ccfe47ad/src/libANGLE/renderer/vulkan/VertexArrayVk.cpp
[modify] https://crrev.com/b97aab3f862af467de71f8b20f87d3e0ccfe47ad/src/tests/gl_tests/IndexBufferOffsetTest.cpp
[modify] https://crrev.com/b97aab3f862af467de71f8b20f87d3e0ccfe47ad/src/libANGLE/renderer/vulkan/ContextVk.h
[modify] https://crrev.com/b97aab3f862af467de71f8b20f87d3e0ccfe47ad/src/libANGLE/renderer/vulkan/ContextVk.cpp

Comment 32 by cclao@google.com on Thu, Mar 10, 2022, 6:46 PM EST Project Member

Alexis, you can land your end2end test now.

Comment 33 by cclao@google.com on Thu, Mar 10, 2022, 6:46 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 34 by Git Watcher on Thu, Mar 10, 2022, 11:00 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5b016f4109f08a3a90ff860c49a68141db6e5d5e

commit 5b016f4109f08a3a90ff860c49a68141db6e5d5e
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Fri Mar 11 03:59:00 2022

Roll ANGLE from 1cfbe863ad52 to b97aab3f862a (1 revision)

https://chromium.googlesource.com/angle/angle.git/+log/1cfbe863ad52..b97aab3f862a

2022-03-10 cclao@google.com Vulkan: resync mCurrentElementArrayBuffer when out of lineloop

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

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 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:1299261~~
Tbr: yuxinhu@google.com
Change-Id: If521ec45c471231d87facd042946584044c7f7b0
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3517888
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@{#980121}

[modify] https://crrev.com/5b016f4109f08a3a90ff860c49a68141db6e5d5e/DEPS

Comment 35 by sheriffbot on Fri, Mar 11, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 36 by sheriffbot on Fri, Mar 11, 2022, 1:42 PM EST Project Member

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

Comment 37 by sheriffbot on Sat, Mar 12, 2022, 2:05 PM EST Project Member

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

Requesting merge to stable M99 because latest trunk commit (980121) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (980121) appears to be after beta branch point (972766).

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

Comment 38 by sheriffbot on Sat, Mar 12, 2022, 2:09 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 OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?

3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

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

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

Comment 39 by sheriffbot on Sat, Mar 12, 2022, 2:09 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 40 by abdolrashidi@google.com on Mon, Mar 14, 2022, 7:44 PM EDT Project Member

Hello,

1. It is a security fix.
2. Link: https://crrev.com/c/3513553
3. Yes. It is already merged to main and rolled in Chromium.
4. No, it is not a new feature.
5. N/A
6. No, security fix tests are automated.

Comment 41 by srinivassista@google.com on Tue, Mar 15, 2022, 1:06 PM EDT Project Member

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

Merge approved for M100 branch: please refer to go/chrome-branches for info

Please complete your merge by 2pm PST today so it can be included in this weeks beta release.

Comment 42 by amyressler@chromium.org on Tue, Mar 15, 2022, 2:41 PM EDT Project Member

Labels: -Merge-Review-99

merge-na-99 as there are no further planned releases of M99 stable
please merge to M100 ASAP/by 2pm PDT today, so this fix can be included in tomorrow's beta release

Comment 43 by cclao@google.com on Tue, Mar 15, 2022, 3:48 PM EDT Project Member

Status: Started (was: Fixed)

Steven Noonan reprted seeing assertions with the landed fix, so I am making revision on the fix. Move back to open now. Also note that this is not a regression bug. This security bug was existed all the time. So take that into account when considering the blocker status.
The revised fix is expected to land this week.

Comment 44 by srinivassista@google.com on Tue, Mar 15, 2022, 4:02 PM EDT Project Member

Cc: amyressler@google.com

thanks cclao@ , i am dropping merge-approved label for now.

amyressler@ please review and update blocker status accordingly

Comment 45 by srinivassista@google.com on Tue, Mar 15, 2022, 4:02 PM EDT Project Member

Labels: -Merge-Approved-100

Comment 46 by amyressler@chromium.org on Tue, Mar 15, 2022, 4:16 PM EDT Project Member

Labels: -ReleaseBlock-Stable

thanks for the insight and working on a fix cclao@

For the record, this was never supposed to be marked as a release-blocker. I've been fighting with the bot over many comments above. We mark it as foundin-98 to make it clear the issue goes back to at least M98, the oldest active release channel. This is not considered a regression nor a release blocker.

Comment 47 by amyressler@chromium.org on Tue, Mar 15, 2022, 4:16 PM EDT Project Member

Cc: -amyressler@google.com amyressler@chromium.org

Comment 48 by Git Watcher on Tue, Mar 15, 2022, 6:22 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/349636a05a3577a127adb6c79a1e947890bbe462

commit 349636a05a3577a127adb6c79a1e947890bbe462
Author: Charlie Lao <cclao@google.com>
Date: Tue Mar 15 16:39:36 2022

Vulkan: Update mCurrentElementArrayBuffersync based on dirty bit

The previous fix crrev.com/c/3513553 has run into corner case that
requires more follow up change crrev.com/c/3522565. But with that, there
is report that now we are hitting assertion in
handleDirtyGraphicsIndexBuffer(). This becomes a bit fragile This new
fix relies on the DIRTY_BIT_INDEX_BUFFER dirty bit and should be more
reliable as long as the dirty bit is set properly (if not, then we have
other bug that it won't even send down vulkan command to bind the
correct element buffer). We could further optimize the code path and

correct element buffer). We could further optimize the code path and
create a fast path for most common usages in the future.

~~Bug: chromium:1299261~~
Change-Id: Ifa8f86d431798c9ca4c128ed71a3e9e0a3537ccb
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3526021
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Charlie Lao <cclao@google.com>

[modify]
https://crrev.com/349636a05a3577a127adb6c79a1e947890bbe462/src/libANGLE/renderer/vulkan/VertexArrayVk.cpp
[modify] https://crrev.com/349636a05a3577a127adb6c79a1e947890bbe462/src/libANGLE/renderer/vulkan/ContextVk.h
[modify] https://crrev.com/349636a05a3577a127adb6c79a1e947890bbe462/src/libANGLE/renderer/vulkan/ContextVk.cpp

Comment 49 by cclao@google.com on Wed, Mar 16, 2022, 7:35 PM EDT Project Member

This should be fixed now with the above CL.

Comment 50 by cclao@google.com on Wed, Mar 16, 2022, 7:36 PM EDT Project Member

Status: Fixed (was: Started)

Comment 51 by Git Watcher on Wed, Mar 16, 2022, 8:46 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9b1219a869bd9b469bac758bc9f8463b1361b52e

commit 9b1219a869bd9b469bac758bc9f8463b1361b52e
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Thu Mar 17 00:45:04 2022

Roll ANGLE from 3739a195c2df to d867ddbbb1b8 (26 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/3739a195c2df..d867ddbbb1b8

2022-03-16 m.maiya@samsung.com Doc: Update supported EGL minor version
2022-03-16 yuxinhu@google.com Revert "Flush the texture staged updates when destroying context share group"
2022-03-16 lubosz.sarnecki@collabora.com FrameCapture: Add override for GlsizeI* types.
2022-03-16 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-16 romanl@google.com angle_system_info_test also exports androidSdkLevel
2022-03-16 romanl@google.com angle_system_info_test passes json via file
2022-03-16 angle-autoroll@skia-public.iam.gserviceaccount.com Roll vulkan-deps from a11411926c31 to 51988dcdccbf (9 revisions)
2022-03-16 yahan@google.com Do not copy parent layer frame position
2022-03-15 cclao@google.com Vulkan: Update mCurrentElementArrayBuffersync based on dirty bit
2022-03-15 yuxinhu@google.com Flush the texture staged updates when destroying context share group
2022-03-15 b.schade@samsung.com Remove invalid validation check on compressed texture formats
2022-03-15 cclao@google.com Vulkan: Handle the case where the bound buffer is empty
2022-03-15 lubosz.sarnecki@collabora.com FrameCapture: Skip invalid VertexAttribPointer calls in MEC.
2022-03-15 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-15 jmadill@chromium.org Vulkan: Temporarily suppress 3 perf counter tests on P6.

2022-03-15 jmadill@chromium.org Revert "Vulkan: VkFormat/DrmFourCC"
2022-03-15 lexa.knyazev@gmail.com Skip no-op base instance draw calls
2022-03-15 lexa.knyazev@gmail.com Fix typo in DrawElementsInstancedBaseVertexBaseInstanceANGLE

2022-03-15 lexa.knyazev@gmail.com Fix typo in DrawElementsInstancedBaseVertexBaseInstanceANGLE
2022-03-15 angle-autoroll@skia-public.iam.gserviceaccount.com Roll Chromium from ffa866a5ae9e to 45902868a797 (562 revisions)
2022-03-15 b.schade@samsung.com Add usage of Spirv through glslang build flag
2022-03-14 kkinnunen@apple.com Add device id as a part of the key in EGLDisplay cache
2022-03-14 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-14 angle-autoroll@skia-public.iam.gserviceaccount.com Roll vulkan-deps from 2d9abfbddc1b to a11411926c31 (18 revisions)
2022-03-14 jmadill@chromium.org Fix crash when pausing XFB then deleting a buffer.
2022-03-14 cclao@google.com Vulkan: Fix another corner case of mCurrentElementArrayBuffer
2022-03-14 angle-autoroll@skia-public.iam.gserviceaccount.com Roll VK-GL-CTS from f7e842466e0a to 8252a3d3cdd3 (8 revisions)

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 jmadill@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 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:1296467~~,~~chromium:1299211~~,~~chromium:1299261~~,~~chromium:1305190~~
Tbr: jmadill@google.com
Test: Test: angle_end2end_tests --gtest_filter="VertexAttributeTestES3.InvalidAttribPointer/*"
Test: Test: capture_replay_tests.py --gtest_filter=FenceSyncTest.NullLength/*
Test: Test: gtest_filter=*DXT1CompressedTextureTest.NonBlockSizesMipLevels*
Test: Test: when using ANGLE (with metal or swiftshader backend) with
Change-Id: I52ffe787d20dd083af8efe1bdef05616ac611f55
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3530116
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@{#981945}

[modify] https://crrev.com/9b1219a869bd9b469bac758bc9f8463b1361b52e/DEPS

Comment 52 by amyressler@google.com on Wed, Mar 23, 2022, 3:46 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

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 53 by amyressler@chromium.org on Wed, Mar 23, 2022, 3:51 PM EDT Project Member

Congratulations, SeongHwan! The VRP Panel has decided to award you $7000 for this report. Thank you for your continued efforts in reporting GPU bugs and nice work!

Comment 54 by amyressler@google.com on Fri, Mar 25, 2022, 5:01 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 55 by abdolrashidi@google.com on Thu, Mar 31, 2022, 6:47 PM EDT Project Member

Owner: cclao@google.com

Comment 56 by amyressler@chromium.org on Fri, Apr 15, 2022, 3:53 PM EDT Project Member

Labels: Merge-Approved-100

In checking the CLs in this bug, both CLs were merged to M101 but neither to M100. As this is a high-severity issue, please merge to M100 so this fix can be included in Extended Stable when M101 is promoted to Stable channel

Please merge both fixes to branch 4896 as soon as possible -- thank you

Comment 57 by sheriffbot on Tue, Apr 19, 2022, 12:19 PM EDT Project Member

Cc: srinivassista@google.com

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 58 by Git Watcher on Thu, Apr 21, 2022, 2:55 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/angle/angle/+/19683d2d5782c58ea50342c7f9c16d2a0138f6ab

commit 19683d2d5782c58ea50342c7f9c16d2a0138f6ab
Author: Charlie Lao <cclao@google.com>
Date: Tue Mar 15 16:39:36 2022

Vulkan: Update mCurrentElementArrayBuffersync based on dirty bit

The previous fix crrev.com/c/3513553 has run into corner case that
requires more follow up change crrev.com/c/3522565. But with that, there
is report that now we are hitting assertion in

is report that now we are hitting assertion in
handleDirtyGraphicsIndexBuffer(). This becomes a bit fragile This new
fix relies on the DIRTY_BIT_INDEX_BUFFER dirty bit and should be more
reliable as long as the dirty bit is set properly (if not, then we have
other bug that it won't even send down vulkan command to bind the
correct element buffer). We could further optimize the code path and
create a fast path for most common usages in the future.

~~Bug: chromium:1299261~~
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3526021
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Charlie Lao <cclao@google.com>
Change-Id: If83cc3f15089bfac42408acd6777c97e944fbaa8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3599604
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Auto-Submit: Charlie Lao <cclao@google.com>

[modify]
https://crrev.com/19683d2d5782c58ea50342c7f9c16d2a0138f6ab/src/libANGLE/renderer/vulkan/VertexArrayVk.cpp
[modify] https://crrev.com/19683d2d5782c58ea50342c7f9c16d2a0138f6ab/src/libANGLE/renderer/vulkan/ContextVk.h
[modify] https://crrev.com/19683d2d5782c58ea50342c7f9c16d2a0138f6ab/src/libANGLE/renderer/vulkan/ContextVk.cpp

Comment 59 by Git Watcher on Thu, Apr 21, 2022, 2:55 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/f8f3b0334397f0f366651a982405fd171d5703fa

commit f8f3b0334397f0f366651a982405fd171d5703fa
Author: Charlie Lao <cclao@google.com>
Date: Mon Mar 14 16:33:28 2022

Vulkan: Fix another corner case of mCurrentElementArrayBuffer

mCurrentElementArrayBuffer is vertex array state. But it gets modified
with different draw call parameters. When this changes, we always
re-calculate mCurrentElementArrayBuffer. And we have added
updateCurrentElementArrayBuffer call at various places where we need to
reset mCurrentElementArrayBuffer to back to what bound to vertex array.
There is still one more places missing such call, that when a different
vertex array is been bound, the new vertex array may still have
mCurrentElementArrayBuffer set to the special array for LineLoop. We
need to reset it upon it gets bound.

This CL also adds a new test case DrawElementsTest.LineLoopTriangles
from Steven Noonan.

~~Bug: chromium:1299261~~
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3522565
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Charlie Lao <cclao@google.com>
Change-Id: Ib8c6a0d7a38351b154a35eb298cb5cc418ccf3b6
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3599603
Reviewed-by: Geoff Lang <geofflang@chromium.org>

Reviewed-by: Geoff Lang <geofflang@chromium.org>
Auto-Submit: Charlie Lao <cclao@google.com>

[modify] https://crrev.com/f8f3b0334397f0f366651a982405fd171d5703fa/src/libANGLE/renderer/vulkan/ContextVk.cpp
[modify] https://crrev.com/f8f3b0334397f0f366651a982405fd171d5703fa/src/tests/gl_tests/DrawElementsTest.cpp

Comment 60 by Git Watcher on Thu, Apr 21, 2022, 2:55 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/b5e0f4b5b96df1289627769dfaf1b04bdf88293c

commit b5e0f4b5b96df1289627769dfaf1b04bdf88293c
Author: Charlie Lao <cclao@google.com>
Date: Thu Mar 10 01:36:24 2022

Vulkan: resync mCurrentElementArrayBuffer when out of lineloop

When glDrawElements is called with GL_UNSIGNED_BYTE type or LineLoop mode, we will internally allocate an element buffer and copy data to it. But when we switch out of that mode, we must re-sync mCurrentElementArrayBuffer to what it should be based on VertexArray buffer binding. This CL fix the bug that we were previously not updating it and end up using the wrong element buffer.

Also added three tests:

DrawWithSameBufferButDifferentTypes: that uses GL_UNSIGNED_BYTE data and GL_UNSIGNED_SHORT data in the same buffer and switch between these two data types without incurring buffer change.

DrawWithSameBufferButDifferentModes: draw line mode followed by triangle without the same element buffer.

DrawArraysLineLoopFollowedByDrawElementsTriangle: draw line mode with glDrawArrays and then followed by DrawElements.

~~Bug: chromium:1299261~~
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3513553
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Commit-Queue: Charlie Lao <cclao@google.com>
Change-Id: Ie15a639740ccb627eab4e0a2770fc1524c0f9aa6
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3599602
Reviewed-by: Geoff Lang <geofflang@chromium.org>

[modify] https://crrev.com/b5e0f4b5b96df1289627769dfaf1b04bdf88293c/src/libANGLE/renderer/vulkan/VertexArrayVk.h
[modify] https://crrev.com/b5e0f4b5b96df1289627769dfaf1b04bdf88293c/src/libANGLE/renderer/vulkan/VertexArrayVk.cpp
[modify] https://crrev.com/b5e0f4b5b96df1289627769dfaf1b04bdf88293c/src/libANGLE/renderer/vulkan/ContextVk.h
[modify] https://crrev.com/b5e0f4b5b96df1289627769dfaf1b04bdf88293c/src/tests/gl_tests/IndexBufferOffsetTest.cpp
[modify] https://crrev.com/b5e0f4b5b96df1289627769dfaf1b04bdf88293c/src/libANGLE/renderer/vulkan/ContextVk.cpp

Comment 61 by sheriffbot on Thu, Apr 21, 2022, 3:00 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?
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 62 by rzanoni@google.com on Mon, Apr 25, 2022, 2:44 PM EDT Project Member

Cc: rzanoni@google.com
Labels: LTS-Merge-Request-96

Comment 63 by sheriffbot on Mon, Apr 25, 2022, 2:50 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 64 by amyressler@chromium.org on Mon, Apr 25, 2022, 8:39 PM EDT Project Member

Labels: Release-0-M101

Comment 65 by rzanoni@google.com on Tue, Apr 26, 2022, 9:47 AM EDT Project Member

1. Just https://crrev.com/c/3605834
2. Low, a few conflicts regarding the way main vs 96 update buffer and buffer offset in ContextVk::syncState
3. Merged to main on Mar 15
4. Yes

Note: there's a failing test, but it also fail without the CL: https://chromium-review.googlesource.com/c/angle/angle/+/3605834/comments/d26be9b8_c3fc7611

Comment 66 by gmpritchard@google.com on Tue, Apr 26, 2022, 10:37 AM EDT Project Member

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

Comment 67 by Git Watcher on Tue, Apr 26, 2022, 1:38 PM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/d27d9d059b51badd1477e029e3b757b478d3140d

commit d27d9d059b51badd1477e029e3b757b478d3140d
Author: Charlie Lao <cclao@google.com>
Date: Tue Mar 15 16:39:36 2022

[M96-LTS] Vulkan: Update mCurrentElementArrayBuffersync based on dirty bit

M96 merge issues:
  ContextVk.cpp:
    ContextVk::setupIndexedDraw: vertexArrayVk/getVertexArray() isn't present in M96
    ContextVk::syncState: M96 uses mVertexArray instead of vertexArrayVk
  VertexArrayVk.cpp:
    VertexArrayVk::updateCurrentElementArrayBuffer doesn't exist in M9
    Created it and kept M96 logic for retrieving buffer/offset

The previous fix crrev.com/c/3513553 has run into corner case that
requires more follow up change crrev.com/c/3522565. But with that, there
is report that now we are hitting assertion in
handleDirtyGraphicsIndexBuffer(). This becomes a bit fragile This new
fix relies on the DIRTY_BIT_INDEX_BUFFER dirty bit and should be more
reliable as long as the dirty bit is set properly (if not, then we have
other bug that it won't even send down vulkan command to bind the
correct element buffer). We could further optimize the code path and
create a fast path for most common usages in the future.

~~Bug: chromium:1299261~~
Change-Id: Ifa8f86d431798c9ca4c128ed71a3e9e0a3537ccb
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3526021
Commit-Queue: Charlie Lao <cclao@google.com>
(cherry picked from commit 349636a05a3577a127adb6c79a1e947890bbe462)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3605834
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Charlie Lao <cclao@google.com>

[modify]
https://crrev.com/d27d9d059b51badd1477e029e3b757b478d3140d/src/libANGLE/renderer/vulkan/VertexArrayVk.h
[modify]
https://crrev.com/d27d9d059b51badd1477e029e3b757b478d3140d/src/libANGLE/renderer/vulkan/VertexArrayVk.cpp
[modify] https://crrev.com/d27d9d059b51badd1477e029e3b757b478d3140d/src/libANGLE/renderer/vulkan/ContextVk.cpp

Comment 68 by amyressler@google.com on Tue, Apr 26, 2022, 4:30 PM EDT Project Member

Labels: CVE-2022-1478 CVE_description-missing

Comment 69 by rzanoni@google.com on Tue, Apr 26, 2022, 4:42 PM EDT Project Member

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

Comment 70 by sheriffbot on Thu, Jun 23, 2022, 1:31 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

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

Comment 71 by carlosil@chromium.org on Fri, Jul 1, 2022, 5:29 PM EDT Project Member

~~Issue 1341203~~ has been merged into this issue.

Comment 72 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 73 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy