☆ Starred by 3 users

Owner:	jmad...@chromium.org
CC:	----
Status:	Fixed *(Closed)*
Components:	Internals>GPU>ANGLE
Modified:	Nov 16, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
reward-9500
M-92
Target-92
external_security_report
merge-merged-4430
merge-merged-90
FoundIn-92
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
LTS-Size-Small
LTS-Complexity-Trivial
Release-2-M92
CVE-2021-30604

Issue 1234829: Security: [ANGLE] Heap use-after-free in TextureD3D::releaseTexStorage

Reported by ggabu...@gmail.com on Fri, Jul 30, 2021, 1:30 PM EDT

Code

[ANGLE] Use-after-free in TextureD3D::releaseTexStorage

VULNERABILITY DETAILS
There is a use-after-free vulnerability that is caused by the TextureD3D::releaseTexStorage function.

RenderTargetCache object caches the RenderTarget object for drawing.
And a TextureD3D object has a TextureStorage object as a member, and a TextureStorage object has a RenderTarget as a member.

TextureD3D::releaseTexStorage function releases the TextureStorage member. At this time, the RenderTarget object is also released.
This RenderTarget object may be referenced by a RenderTargetCache object.
Therefore, the releaseTexStorage function must set the DirtyBit to update the RenderTargetCache object.

But it doesn't exist in current code like this:

```
------------------------------------------------------------------------------------------------
angle::Result TextureD3D::releaseTexStorage(const gl::Context *context)
{
    if (!mTexStorage)
    {
        return angle::Result::Continue;
    }

    auto err = mTexStorage->onDestroy(context);
    SafeDelete(mTexStorage);
    return err;
}
------------------------------------------------------------------------------------------------
```

So the following code will get a pointer to a RenderTarget object that has already been freed.

```
------------------------------------------------------------------------------------------------
RenderTarget11 *Framebuffer11::getFirstRenderTarget() const
{
    for (auto *renderTarget : mRenderTargetCache.getColors())
    {
        if (renderTarget)
        {
            return renderTarget;
        }
    }

    return mRenderTargetCache.getDepthStencil();
}
------------------------------------------------------------------------------------------------
```

The attached PoC reallocates the Buffer to the freed RenderTarget object memory.
The debugger outputs the following exception:

```
-----------------------------------------------------------------------------------------------
libglesv2!rx::StateManager11::updateState+0x101:
00007ffb`bce69071 ff5228          call    qword ptr [rdx+28h] ds:77777777`7777779f=????????????????
0:000> !heap -p -a @rax
    address 00000170ed18b1b0 found in
    _HEAP @ 170ea7e0000
              HEAP_ENTRY Size Prev Flags            UserPtr UserSize - state
        00000170ed18b180 000e 0000  [00]   00000170ed18b1b0    000b0 - (busy)
          unknown!printable
        7ffbf3a5b49d ntdll!RtlpAllocateHeapInternal+0x0000000000000a7d
        7ffbbd0e8eac libglesv2!_malloc_base+0x0000000000000044
        7ffbbd057c48 libglesv2!angle::MemoryBuffer::resize+0x0000000000000028
        7ffbbce3d73a libglesv2!rx::Buffer11::SystemMemoryStorage::resize+0x000000000000002a
        7ffbbce39df6 libglesv2!rx::Buffer11::setSubData+0x0000000000000526
        7ffbbce3971b libglesv2!rx::Buffer11::setData+0x000000000000004b
        7ffbbccdd2f3 libglesv2!rx::BufferImpl::setDataWithUsageFlags+0x0000000000000023
        7ffbbcc27411 libglesv2!gl::Buffer::bufferDataImpl+0x0000000000000111
        7ffbbcc274f3 libglesv2!gl::Buffer::bufferData+0x0000000000000023
        7ffbbcc4bc76 libglesv2!gl::Context::bufferData+0x0000000000000046
        7ffbbcbd2d44 libglesv2!GL_BufferData+0x00000000000000b4
-----------------------------------------------------------------------------------------------
```

VERSION

Chrome Version: master (and tested on 92.0.4515.107 (Official Build) (64-bit) Stable)
Operating System: Windows 10 x64

REPRODUCTION CASE

Run the attached poc.html

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash: GPU Process
Crash State:

```
=================================================================
==9072==ERROR: AddressSanitizer: heap-use-after-free on address 0x11a8c1a56be0 at pc 0x7ffb79542db0 bp 0x0088c7dfe680 sp 0x0088c7dfe6c8
READ of size 8 at 0x11a8c1a56be0 thread T0
==9072==WARNING: Failed to use and restart external symbolizer!
==9072==*** WARNING: Failed to initialize DbgHelp!              ***
==9072==*** Most likely this means that the app is already      ***
==9072==*** using DbgHelp, possibly with incompatible flags.    ***
==9072==*** Due to technical reasons, symbolization might crash ***
==9072==*** or produce wrong results.                           ***
    #0 0x7ffb79542daf in rx::StateManager11::updateState C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\StateManager11.cpp:2208
    #1 0x7ffb794c5452 in rx::Context11::drawArrays C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Context11.cpp:268
    #2 0x7ffb78f3d9ad in GL_DrawArrays C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:1063
    #3 0x7ffb8fedb746 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:1210
    #4 0x7ffb8c153c53 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:858
    #5 0x7ffb8c1530b0 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:796
    #6 0x7ffb89176d8e in gpu::CommandBufferService::Flush C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #7 0x7ffb868cc414 in gpu::CommandBufferStub::OnAsyncFlush C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:498
    #8 0x7ffb868cb5c8 in gpu::CommandBufferStub::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:149
    #9 0x7ffb868d82e4 in gpu::GpuChannel::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:666
    #10 0x7ffb868e340d in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::DeferredRequestParams> >,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #11 0x7ffb86509970 in gpu::Scheduler::RunNextTask C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:688
    #12 0x7ffb852ede7a in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:178
    #13 0x7ffb87c99892 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:360
    #14 0x7ffb87c98ef2 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:260
    #15 0x7ffb87c6db87 in base::MessagePumpDefault::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
    #16 0x7ffb87c9ad8e 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:467
    #17 0x7ffb852701e3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:134
    #18 0x7ffb876ccb86 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:428
    #19 0x7ffb810ba701 in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:973
    #20 0x7ffb810b715a in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:390
    #21 0x7ffb810b819c in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:418
    #22 0x7ffb7aab145a in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:168
    #23 0x7ff6bf665b74 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #24 0x7ff6bf662be8 in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #25 0x7ff6bfa5132f in __scrt_common_main_seh d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #26 0x7ffbf3897033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #27 0x7ffbf3a82650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x11a8c1a56be0 is located 0 bytes inside of 176-byte region [0x11a8c1a56be0,0x11a8c1a56c90)
freed by thread T0 here:
    #0 0x7ff6bf705fab in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffb794fef2f in rx::TextureRenderTarget11::~TextureRenderTarget11
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\RenderTarget11.cpp:262
    #2 0x7ffb7956820e in rx::TextureStorage11_2D::~TextureStorage11_2D
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\TextureStorage11.cpp:1066
    #3 0x7ffb79584d0f in rx::TextureStorage11_2D::~TextureStorage11_2D
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\TextureStorage11.cpp:1066
    #4 0x7ffb7960f084 in rx::TextureD3D::setBaseLevel C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\TextureD3D.cpp:692
    #5 0x7ffb7911db79 in gl::Texture::setBaseLevel C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Texture.cpp:1008
    #6 0x7ffb7917f699 in gl::`anonymous namespace'::SetTexParameterBase<0,0,int> C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\queryutils.cpp:443
    #7 0x7ffb7917f0bd in gl::SetTexParameteri C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\queryutils.cpp:1769
    #8 0x7ffb78f4411d in GL_TexParameteri C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:2867
    #9 0x7ffb8feec28c in gpu::gles2::GLES2DecoderPassthroughImpl::DoTexParameteri
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:2805
    #10 0x7ffb8c153c53 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:858
    #11 0x7ffb8c1530b0 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:796
    #12 0x7ffb89176d8e in gpu::CommandBufferService::Flush C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #13 0x7ffb868cc414 in gpu::CommandBufferStub::OnAsyncFlush C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:498
    #14 0x7ffb868cb5c8 in gpu::CommandBufferStub::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:149
    #15 0x7ffb868d82e4 in gpu::GpuChannel::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:666
    #16 0x7ffb868e340d in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::DeferredRequestParams> >,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #17 0x7ffb86509970 in gpu::Scheduler::RunNextTask C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:688
    #18 0x7ffb852ede7a in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:178
    #19 0x7ffb87c99892 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:360
    #20 0x7ffb87c98ef2 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:260
    #21 0x7ffb87c6db87 in base::MessagePumpDefault::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
    #22 0x7ffb87c9ad8e 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:467
    #23 0x7ffb852701e3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:134
    #24 0x7ffb876ccb86 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:428
    #25 0x7ffb810ba701 in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:973
    #26 0x7ffb810b715a in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:390
    #27 0x7ffb810b819c in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:418

previously allocated by thread T0 here:
    #0 0x7ff6bf7060ab in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffb79d81dfe in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffb7956a575 in rx::TextureStorage11_2D::getRenderTarget
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\TextureStorage11.cpp:1406
    #3 0x7ffb7960e966 in rx::TextureD3D::getAttachmentRenderTarget C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\TextureD3D.cpp:647
    #4 0x7ffb794dfe61 in rx::RenderTargetCache<rx::RenderTarget11>::updateCachedRenderTarget
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\RenderTargetCache.h:163
    #5 0x7ffb794dfcb5 in rx::RenderTargetCache<rx::RenderTarget11>::updateColorRenderTarget
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\RenderTargetCache.h:137
    #6 0x7ffb794dfa64 in rx::RenderTargetCache<rx::RenderTarget11>::update C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\RenderTargetCache.h:97
    #7 0x7ffb794df894 in rx::Framebuffer11::syncState C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Framebuffer11.cpp:398
    #8 0x7ffb79038ef7 in gl::Framebuffer::syncState C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Framebuffer.cpp:2051
    #9 0x7ffb7910d9a4 in gl::State::syncDirtyObject C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\State.cpp:3410
    #10 0x7ffb78fe05fb in gl::Context::invalidateFramebuffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:4729
    #11 0x7ffb78f4eca8 in GL_InvalidateFramebuffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_3_0_autogen.cpp:1663
    #12 0x7ffb8fee663f in gpu::gles2::GLES2DecoderPassthroughImpl::DoInvalidateFramebuffer
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:2244
    #13 0x7ffb8c153c53 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:858
    #14 0x7ffb8c1530b0 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:796
    #15 0x7ffb89176d8e in gpu::CommandBufferService::Flush C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #16 0x7ffb868cc414 in gpu::CommandBufferStub::OnAsyncFlush C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:498
    #17 0x7ffb868cb5c8 in gpu::CommandBufferStub::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:149
    #18 0x7ffb868d82e4 in gpu::GpuChannel::ExecuteDeferredRequest C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:666
    #19 0x7ffb868e340d in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::DeferredRequestParams> >,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #20 0x7ffb86509970 in gpu::Scheduler::RunNextTask C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:688
    #21 0x7ffb852ede7a in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:178
    #22 0x7ffb87c99892 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:360
    #23 0x7ffb87c98ef2 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:260
    #24 0x7ffb87c6db87 in base::MessagePumpDefault::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:39
    #25 0x7ffb87c9ad8e 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:467
    #26 0x7ffb852701e3 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:134
    #27 0x7ffb876ccb86 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:428

SUMMARY: AddressSanitizer: heap-use-after-free C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\StateManager11.cpp:2208 in
rx::StateManager11::updateState
Shadow bytes around the buggy address:
  0x03bfd9d4ad20: fa fa fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x03bfd9d4ad30: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x03bfd9d4ad40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x03bfd9d4ad50: fd fd fd fd fd fa fa fa fa fa fa fa fa fa fd fd
  0x03bfd9d4ad60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x03bfd9d4ad70: fd fd fd fd fa fa fa fa fa fa fa fa[fd]fd fd fd
  0x03bfd9d4ad80: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x03bfd9d4ad90: fd fd fa fa fa fa fa fa fa fa 00 00 00 00 00 00
  0x03bfd9d4ada0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x03bfd9d4adb0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x03bfd9d4adc0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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
==9072==ABORTING
[3968:3752:0731/003258.174:ERROR:gpu_process_host.cc(951)] GPU process exited unexpectedly: exit_code=1
```

CREDIT INFORMATION

Reporter credit: Seong-Hwan Park (SeHwa) of SecunologyLab

poc.html
2.0 KB View Download

Comment 1 by sheriffbot on Fri, Jul 30, 2021, 1:31 PM EDT Project Member

Labels: external_security_report

Comment 2 by ggabu...@gmail.com on Fri, Jul 30, 2021, 1:41 PM EDT

Here is the patch: https://crrev.com/c/3063858

Comment 3 by meacer@google.com on Mon, Aug 2, 2021, 6:29 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: jmad...@chromium.org
Labels: Security_Severity-High Security_Impact-Stable FoundIn-92 OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: Internals>GPU>ANGLE

Thanks for the report.

jmadill: Could you PTAL?

Comment 4 by sheriffbot on Mon, Aug 2, 2021, 12:47 PM EDT Project Member

Labels: M-92 Target-92

Setting milestone and target because of high severity.

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

Comment 5 by Git Watcher on Fri, Aug 6, 2021, 2:53 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/16a61bbbde1f64e39e88b58ac68f5567893a181c

commit 16a61bbbde1f64e39e88b58ac68f5567893a181c
Author: SeongHwan Park <ggabu423@gmail.com>
Date: Thu Aug 05 14:06:22 2021

D3D: Fix not notifying RenderTarget release in TextureD3D

This could lead to use-after-free for the RenderTarget object.

~~Bug: chromium:1234829~~
Change-Id: I73d4547b8f09f2f2cf3f7f8394f7f573fe5a4ef5
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3063858
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/16a61bbbde1f64e39e88b58ac68f5567893a181c/src/libANGLE/Framebuffer.cpp
[modify] https://crrev.com/16a61bbbde1f64e39e88b58ac68f5567893a181c/src/libANGLE/Observer.h
[modify] https://crrev.com/16a61bbbde1f64e39e88b58ac68f5567893a181c/src/libANGLE/Texture.cpp
[modify] https://crrev.com/16a61bbbde1f64e39e88b58ac68f5567893a181c/src/libANGLE/renderer/d3d/TextureD3D.cpp
[modify] https://crrev.com/16a61bbbde1f64e39e88b58ac68f5567893a181c/src/tests/gl_tests/TextureTest.cpp

Comment 6 by Git Watcher on Fri, Aug 6, 2021, 5:53 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e24e07aa7710da5a8b523fddf9d672ced8023113

commit e24e07aa7710da5a8b523fddf9d672ced8023113
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Fri Aug 06 21:52:13 2021

Roll ANGLE from 89dbbb2ac687 to 16a61bbbde1f (6 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/89dbbb2ac687..16a61bbbde1f

2021-08-06 ggabu423@gmail.com D3D: Fix not notifying RenderTarget release in TextureD3D
2021-08-06 cclao@google.com Vulkan: Add test for BufferData change is propagated to SSBO properly
2021-08-06 cclao@google.com Vulkan: Propagate BufferData changes to atomic counter binding
2021-08-06 angle-autoroll@skia-public.iam.gserviceaccount.com Roll Chromium from 3d40e0a2ae46 to 54236e566eab (96 revisions)
2021-08-06 cclao@google.com Vulkan: Test for buffer storage propagate to AtomicCounter properly
2021-08-06 lubosz.sarnecki@collabora.com PerfTests: Replay EGL color spaces.

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 syoussefi@google.com on the revert to ensure that a human
is aware of the problem.

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-asan;luci.chromium.try:win_optional_gpu_tests_rel;luci.chromium.try:linux-swangle-try-x64;luci.chromium.try:win-swangle-try-x86
~~Bug: chromium:1234829~~
Tbr: syoussefi@google.com
Change-Id: Ic77368a8d9478b7e5a29c646839a7d177485d2dd
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3076978

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/master@{#909495}

[modify] https://crrev.com/e24e07aa7710da5a8b523fddf9d672ced8023113/DEPS

Comment 7 by jmad...@chromium.org on Tue, Aug 10, 2021, 11:22 AM EDT Project Member

Status: Fixed (was: Assigned)

Comment 8 by sheriffbot on Tue, Aug 10, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 9 by sheriffbot on Tue, Aug 10, 2021, 1:41 PM EDT Project Member

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

Comment 10 by sheriffbot on Tue, Aug 10, 2021, 2:01 PM EDT Project Member

Labels: Merge-Request-92 Merge-Request-93

Requesting merge to stable M92 because latest trunk commit (909495) appears to be after stable branch point (885287).

Requesting merge to beta M93 because latest trunk commit (909495) appears to be after beta branch point (902210).

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

Comment 11 by sheriffbot on Tue, Aug 10, 2021, 2:03 PM EDT Project Member

Labels: -Merge-Request-93 Hotlist-Merge-Review Merge-Review-93

This bug requires manual review: DEPS changes referenced in bugdroid comments.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/main/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

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

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

Comment 12 by jmad...@chromium.org on Tue, Aug 10, 2021, 2:26 PM EDT Project Member

1. yes
2. https://chromium-review.googlesource.com/c/angle/angle/+/3063858
3. yes
4. M92
5. use-after-free fix
6. no
7. n/a

Comment 13 by amyressler@google.com on Tue, Aug 10, 2021, 2:58 PM EDT Project Member

Labels: -Merge-Request-92 -Merge-Review-93 Merge-Approved-92 Merge-Approved-93

Approved to merge to M92 and M93, please merge to branch 4577 (for M93) by EOD today if at all possible, so it can be a part of tomorrow's beta release.
Please merge to branch M92/branch 4515 by 5pm PDT Thursday so it can be a part of next week's M92 security refresh. Thank you!

Comment 14 by Git Watcher on Tue, Aug 10, 2021, 3:18 PM EDT Project Member

Labels: -merge-approved-93 merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/f42bd00efd49b8163399c2ebd62511f4a5106aaf

commit f42bd00efd49b8163399c2ebd62511f4a5106aaf
Author: SeongHwan Park <ggabu423@gmail.com>
Date: Thu Aug 05 14:06:22 2021

D3D: Fix not notifying RenderTarget release in TextureD3D

This could lead to use-after-free for the RenderTarget object.

~~Bug: chromium:1234829~~
Change-Id: I73d4547b8f09f2f2cf3f7f8394f7f573fe5a4ef5
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3063858
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 16a61bbbde1f64e39e88b58ac68f5567893a181c)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3086327

[modify] https://crrev.com/f42bd00efd49b8163399c2ebd62511f4a5106aaf/src/libANGLE/Framebuffer.cpp
[modify] https://crrev.com/f42bd00efd49b8163399c2ebd62511f4a5106aaf/src/libANGLE/Observer.h
[modify] https://crrev.com/f42bd00efd49b8163399c2ebd62511f4a5106aaf/src/libANGLE/Texture.cpp
[modify] https://crrev.com/f42bd00efd49b8163399c2ebd62511f4a5106aaf/src/libANGLE/renderer/d3d/TextureD3D.cpp
[modify] https://crrev.com/f42bd00efd49b8163399c2ebd62511f4a5106aaf/src/tests/gl_tests/TextureTest.cpp

Comment 15 by Git Watcher on Tue, Aug 10, 2021, 3:19 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9

commit f11eb737212f1f5e733d259a0a0dd2ff24dea2b9
Author: SeongHwan Park <ggabu423@gmail.com>
Date: Thu Aug 05 14:06:22 2021

D3D: Fix not notifying RenderTarget release in TextureD3D

This could lead to use-after-free for the RenderTarget object.

~~Bug: chromium:1234820~~
Change-Id: I73d4547b8f09f2f2cf3f7f8394f7f573fe5a4ef5
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3063858
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 16a61bbbde1f64e39e88b58ac68f5567893a181c)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3086328

[modify] https://crrev.com/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9/src/libANGLE/Framebuffer.cpp
[modify] https://crrev.com/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9/src/libANGLE/Observer.h
[modify] https://crrev.com/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9/src/libANGLE/Texture.cpp
[modify] https://crrev.com/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9/src/libANGLE/renderer/d3d/TextureD3D.cpp
[modify] https://crrev.com/f11eb737212f1f5e733d259a0a0dd2ff24dea2b9/src/tests/gl_tests/TextureTest.cpp

Comment 16 by Git Watcher on Fri, Aug 13, 2021, 2:36 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/bf4eb2636ebae19cfa8d3edb9828bdb464360df5

commit bf4eb2636ebae19cfa8d3edb9828bdb464360df5
Author: Yuly Novikov <ynovikov@chromium.org>
Date: Fri Aug 13 18:09:14 2021

Skip UpdateRenderTargetCacheOnDestroyTexStorage on Metal

Fails in M92 branch, e.g.
https://ci.chromium.org/ui/p/chromium-m92/builders/try/mac_optional_gpu_tests_rel/67/overview

~~Bug: chromium:1234820~~
Change-Id: I74b9694a16fccc4ba358db5dc1168cf9e21ecab0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3094707
Reviewed-by: Yuly Novikov <ynovikov@chromium.org>
Commit-Queue: Yuly Novikov <ynovikov@chromium.org>

[modify] https://crrev.com/bf4eb2636ebae19cfa8d3edb9828bdb464360df5/src/tests/angle_end2end_tests_expectations.txt

Comment 17 by Git Watcher on Fri, Aug 13, 2021, 2:49 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/728baa5089f889dc325f5e3bd4fd6630cbe2c605

commit 728baa5089f889dc325f5e3bd4fd6630cbe2c605
Author: Yuly Novikov <ynovikov@chromium.org>
Date: Fri Aug 13 18:47:50 2021

Revert "Skip UpdateRenderTargetCacheOnDestroyTexStorage on Metal"

This reverts commit bf4eb2636ebae19cfa8d3edb9828bdb464360df5.

Reason for revert: branch created before
angle_end2end_tests_expectations.txt existed,
need to use the old-fashioned suppression method.

Original change's description:
> Skip UpdateRenderTargetCacheOnDestroyTexStorage on Metal
>
> Fails in M92 branch, e.g.
> https://ci.chromium.org/ui/p/chromium-m92/builders/try/mac_optional_gpu_tests_rel/67/overview
>
> ~~Bug: chromium:1234820~~
> Change-Id: I74b9694a16fccc4ba358db5dc1168cf9e21ecab0
> Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3094707
> Reviewed-by: Yuly Novikov <ynovikov@chromium.org>
> Commit-Queue: Yuly Novikov <ynovikov@chromium.org>

~~Bug: chromium:1234820~~
Change-Id: Ifd01947e0ae79619cec3290e4afe1489933a650e
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3093248
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Yuly Novikov <ynovikov@chromium.org>

[modify] https://crrev.com/728baa5089f889dc325f5e3bd4fd6630cbe2c605/src/tests/angle_end2end_tests_expectations.txt

Comment 18 by Git Watcher on Fri, Aug 13, 2021, 3:06 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/6c13370af51bd4a67138aca0b066b102cba1fe15

commit 6c13370af51bd4a67138aca0b066b102cba1fe15
Author: Yuly Novikov <ynovikov@chromium.org>
Date: Fri Aug 13 18:54:49 2021

Remove Texture2DTestES3.UpdateRenderTargetCacheOnDestroyTexStorage

Crashes on Mac Metal in M92 branch, e.g.
https://ci.chromium.org/ui/p/chromium-m92/builders/try/mac_optional_gpu_tests_rel/67/overview

~~Bug: chromium:1234820~~
Change-Id: Icdad981463a50c96c7604a6157107015d18c388f
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3094711
Reviewed-by: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/6c13370af51bd4a67138aca0b066b102cba1fe15/src/tests/gl_tests/TextureTest.cpp

Comment 19 by Git Watcher on Sat, Aug 14, 2021, 1:16 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4b9a038fa410e5f4f03327451dafe545ad449702

commit 4b9a038fa410e5f4f03327451dafe545ad449702
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Sat Aug 14 05:15:53 2021

Roll ANGLE from 201960e4aa83 to 1fb846cbed19 (8 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/201960e4aa83..1fb846cbed19

2021-08-13 lexa.knyazev@gmail.com Validate texStorage dimensions with compressed formats
2021-08-13 kbr@chromium.org In WebGL, constrain base level of compressed textures.
2021-08-13 ynovikov@chromium.org Revert "Skip UpdateRenderTargetCacheOnDestroyTexStorage on Metal"
2021-08-13 ynovikov@chromium.org Skip UpdateRenderTargetCacheOnDestroyTexStorage on Metal
2021-08-13 angle-autoroll@skia-public.iam.gserviceaccount.com Roll VK-GL-CTS from bf3d63599bad to 7103920041db (7 revisions)
2021-08-13 angle-autoroll@skia-public.iam.gserviceaccount.com Roll vulkan-deps from 20a966e2b2fd to 4d36e22f8cc6 (6 revisions)
2021-08-13 angle-autoroll@skia-public.iam.gserviceaccount.com Roll SwiftShader from b2af6a85583d to 526b987888fb (1 revision)
2021-08-13 angle-autoroll@skia-public.iam.gserviceaccount.com Roll Chromium from 5a1d66a9d8fb to 30bbd66599a2 (82 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 ynovikov@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-asan;luci.chromium.try:win_optional_gpu_tests_rel;luci.chromium.try:linux-swangle-try-x64;luci.chromium.try:win-swangle-try-x86
~~Bug: chromium:1234829~~
Tbr: ynovikov@google.com
Change-Id: I3af89fab308efb6b9df4792f3cd9944150f7d3e3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3095126
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/master@{#911981}

[modify] https://crrev.com/4b9a038fa410e5f4f03327451dafe545ad449702/DEPS

Comment 20 by amyressler@google.com on Mon, Aug 16, 2021, 10:10 AM EDT Project Member
Labels: Release-2-M92

Comment 21 by amyressler@google.com on Mon, Aug 16, 2021, 10:20 AM EDT Project Member
Labels: CVE-2021-30604 CVE_description-missing

Comment 22 by rzanoni@google.com on Tue, Aug 17, 2021, 7:13 AM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 23 by amyressler@google.com on Wed, Aug 18, 2021, 7:45 PM EDT Project Member
Labels: -reward-topanel reward-unpaid reward-9500

*** 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 24 by amyressler@chromium.org on Wed, Aug 18, 2021, 8:00 PM EDT Project Member
Congratulations, Seong-Hwan! The VRP Panel has decided to award you $9500 for this report, for your report of this UAF bug in ANGLE + patch bonus. Nice work!

Comment 25 by rzanoni@google.com on Thu, Aug 19, 2021, 11:27 AM EDT Project Member
Labels: LTS-Size-Small LTS-Complexity-Trivial

Comment 26 by amyressler@google.com on Thu, Aug 19, 2021, 6:44 PM EDT Project Member
Labels: -reward-unpaid reward-inprocess

Comment 27 by gianluca@google.com on Fri, Aug 20, 2021, 3:28 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 28 by jmad...@chromium.org on Fri, Aug 20, 2021, 6:55 AM EDT Project Member
What's the branch number for M90? Does the merge process work as for other release branches?

Comment 29 by asumaneev@google.com on Mon, Aug 23, 2021, 7:38 AM EDT Project Member
M90 is LTS branch and is different from regular branches: go/chromeos-commercial-lts-g3doc.

Comment 30 by amyressler@google.com on Thu, Aug 26, 2021, 1:44 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 31 by Git Watcher on Fri, Aug 27, 2021, 7:30 AM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/2ca943d9a2cbd9feb65019c4b864533781047e35

commit 2ca943d9a2cbd9feb65019c4b864533781047e35
Author: SeongHwan Park <ggabu423@gmail.com>

Date: Thu Aug 05 14:06:22 2021

[M90-LTS] D3D: Fix not notifying RenderTarget release in TextureD3D

This could lead to use-after-free for the RenderTarget object.

~~Bug: chromium:1234829~~
Change-Id: I73d4547b8f09f2f2cf3f7f8394f7f573fe5a4ef5
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3063858
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 16a61bbbde1f64e39e88b58ac68f5567893a181c)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3097381
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Geoff Lang <geofflang@chromium.org>

[modify] https://crrev.com/2ca943d9a2cbd9feb65019c4b864533781047e35/src/libANGLE/Framebuffer.cpp
[modify] https://crrev.com/2ca943d9a2cbd9feb65019c4b864533781047e35/src/libANGLE/Observer.h
[modify] https://crrev.com/2ca943d9a2cbd9feb65019c4b864533781047e35/src/libANGLE/Texture.cpp
[modify] https://crrev.com/2ca943d9a2cbd9feb65019c4b864533781047e35/src/libANGLE/renderer/d3d/TextureD3D.cpp
[modify] https://crrev.com/2ca943d9a2cbd9feb65019c4b864533781047e35/src/tests/gl_tests/TextureTest.cpp

Comment 32 by rzanoni@google.com on Fri, Aug 27, 2021, 7:33 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 33 by sheriffbot on Tue, Nov 16, 2021, 1:32 PM EST 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