Google Chrome WebGL Buffer11::getBufferStorage Code Execution Vulnerability

October 20, 2020

https://piotrbania.com

TALOS-2020-1127

CVE Number

CVE-2020-6542

Summary

A code execution vulnerability exists in the WebGL functionality of Google Chrome 84.0.4147.89 and 85.0.4169.0 (Developer Build) (64-bit). A specially crafted web page can cause a use-after-free condition. An attacker can create a special website to trigger this vulnerability.

Tested Versions

Google Chrome Google Chrome 84.0.4147.89

Google Chrome Google Chrome 85.0.4169.0 (Developer Build) (64-bit)

Product URLs

https://www.google.com/chrome/

CVSSv3 Score

8.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L

CWE

CWE-416 - Use After Free

Details

Google Chrome is a cross-platform web browser developed by Google. It supports many features, including WebGL (Web Graphics Library), a JavaScript API for rendering interactive 2-D and 3-D graphics.

This vulnerability happens in ANGLE library (compatibility layer between OpenGL and Direct3D) used by Google Chrome browser.

While running the supplied PoC, Chromium crashes inside the Buffer11::getBufferStorage function. This is because newStorage element points to previously freed memory, leading to a use-after-free vulnerability.

Below is the Buffer11::getBufferStorage function:

```
template <typename StorageOutT>
angle::Result Buffer11::getBufferStorage(const gl::Context *context,
                                         BufferUsage
usage,
                                         StorageOutT
**storageOut)
{
        ASSERT(0 <= usage && usage < BUFFER_USAGE_COUNT);
        BufferStorage *&newStorage = mBufferStorages[usage];                    <--
memory regions already freed
        if (!newStorage)
        {
                newStorage = allocateStorage(usage);
        }
        markBufferUsage(usage);
        // resize buffer
        if (newStorage->getSize() < mSize)
                <-- use after free and below
        {
                ANGLE_TRY(newStorage->resize(context, mSize, true));
        }
        ASSERT(newStorage);
        ANGLE_TRY(updateBufferStorage(context, newStorage, 0, mSize));
        ANGLE_TRY(garbageCollection(context, usage));
        *storageOut = GetAs<StorageOutT>(newStorage);
        return angle::Result::Continue;
}
```

mBufferStorages is defined as a global std:array variable:

```
std::array<BufferStorage *, BUFFER_USAGE_COUNT> mBufferStorages;
```

And it is freed in class destructor:

```
/* libANGLE/renderer/d3d/d3d11/Buffer11.cpp : 356 */
Buffer11::~Buffer11()
{
        for (BufferStorage *&storage : mBufferStorages)
        {
                SafeDelete(storage);
        }
...
}
```

Debugger output:

```
*** WARNING: Unable to verify checksum for
J:\chromium_build\chromium\src\out\Default\libglesv2.dll
libglesv2!rx::Buffer11::BufferStorage::getSize+0x9:
00007ffa`bfe85a79 488b4020        mov     rax,qword ptr [rax+20h]
ds:dddddddd`ddddddfd=????????????????
```

Information from ASAN build:

```
SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer11.cp
p:809:10 in rx::Buffer11::getBufferStorage<class rx::Buffer11::BufferStorage>(class
gl::Context const *, enum rx::BufferUsage, class rx::Buffer11::BufferStorage **)
Shadow bytes around the buggy address:
  0x0411855a4190: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0411855a41a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0411855a41b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

Memory region was initialized here:

```
previously allocated by thread T0 here:
#0 0x7ff6b362d084 in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_malloc_win.cpp:98
#1 0x7ff89b68c652 in operator new(unsigned __int64)
d:\agent\_work\3\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
#2 0x7ff89a8edb23 in rx::Context11::createBuffer(class gl::BufferState const &)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Context11.c
pp:192:24
#3 0x7ff89a4f6bb3 in gl::Buffer::Buffer(class rx::GLImplFactory *, struct gl::BufferID)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:43:22
#4 0x7ff89a645879 in gl::BufferManager::AllocateNewObject(class rx::GLImplFactory *,
struct gl::BufferID)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:127:26
#5 0x7ff89a493af7 in gl::TypedResourceManager<class gl::Buffer, class gl::HandleAllocator,
class gl::BufferManager, struct gl::BufferID>::checkObjectAllocationImpl<>(class
```

rx::GLImplFactory *, struct gl::BufferID)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.h:113:32
#6 0x7ff89a4860f9 in gl::BindBuffer(unsigned int, unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autoge
n.cpp:100:22
...

And freed here:

freed by thread T0 here:
#0 0x7ff6b362cf84 in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-
rt\lib\asan\asan_malloc_win.cpp:82
#1 0x7ff89a8e31bb in rx::Buffer11::`scalar deleting dtor'(unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer11.cp
p:357:1
#2 0x7ff89a4f6dc9 in gl::Buffer::~Buffer(void)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:51:5
#3 0x7ff89a4f7dcd in gl::Buffer::`scalar deleting dtor'(unsigned int)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:50:1
#4 0x7ff89a641629 in gl::TypedResourceManager<class gl::Buffer, class
gl::HandleAllocator, class gl::BufferManager, struct gl::BufferID>::deleteObject(class
gl::Context const *, struct gl::BufferID)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:100:9
#5 0x7ff89a557c39 in gl::Context::deleteBuffers(int, struct gl::BufferID const *)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:6054:9
#6 0x7ff89a488c02 in gl::DeleteBuffers(int, unsigned int const *)
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autoge
n.cpp:695:22
...

Stack trace:

3:033> kb
RetAddr : Args to Child : Call Site
00 00007ffa`bfe88786 : 00000273`ad4c3be0 00000273`a8a0ba60 0000008f`219fb660
00007ffb`782dec50 : libglesv2!rx::Buffer11::BufferStorage::getSize+0x9
[j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer1
1.cpp @ 115]
01 00007ffa`bfe8851a : 00000000`ad6d1730 00007ffa`bf96c889 00000273`a8a0ba60
00000000`00008000 :
libglesv2!rx::Buffer11::getBufferStorage<rx::Buffer11::NativeStorage>+0x1f6
[j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer1
1.cpp @ 817]
02 00007ffa`bff39609 : 00000273`a8d45888 0000008f`219fbda8 01000000`00000010
00007ffa`bf996d00 : libglesv2!rx::Buffer11::getBuffer+0x6a

[j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer11.cpp @ 698]
03 00007ffa`bff32e43 : 0000008f`219fbf08 0000008f`219fbf08 0000008f`219fc338 00007ffa`bf96a39d : libglesv2!rx::StateManager11::applyVertexBuffers+0x8b9 [j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\StateManager11.cpp @ 3082]
04 00007ffa`bff30dd6 : 00000273`a89ed8b0 00000273`ad953200 00000273`ad956010 00000000`00000000 : libglesv2!rx::StateManager11::syncVertexBuffersAndInputLayout+0x433 [j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\StateManager11.cpp @ 3018]
05 00007ffa`bfea121d : 000040cb`d408ccef 00007ffa`bf7f800a 00007ffa`c0a04b10 00000273`ad956618 : libglesv2!rx::StateManager11::updateState+0xfd6 [j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\StateManager11.cpp @ 2327]
06 00007ffa`bf7e67f2 : 00000273`ad953200 00000010`01bff74c 0100008f`00000004 00007ffa`bf7e66f7 : libglesv2!rx::Context11::drawArrays+0x21d [j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Context11.cpp @ 267]
07 00007ffa`bf7e6667 : 00000000`00000001 0000008f`219fc800 00007ffa`c0972971 00000000`00000008 : libglesv2!gl::Context::drawArrays+0xe2 [j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\Context.inl.h @ 120]
08 00007ffa`bf8d95e3 : 00000273`ad5719d8 00000001`219fc908 00000001`00000001 00000001`00000004 : libglesv2!gl::DrawArrays+0x167 [j:\chromium_build\chromium\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp @ 929]
09 00007ffa`d1de5226 : 00000273`a8ea0f00 00000273`a8ea0f04 00000273`a8ea0dc0 00000273`a8ea0dc0 : libglesv2!glDrawArrays+0x23 [j:\chromium_build\chromium\src\third_party\angle\src\libGLESv2\libGLESv2_autogen.cpp @ 260]
0a 00007ffa`d1e619f9 : 00000273`ad5221e0 00007ffa`c9d4fc32 00000273`ad1d1590 00007ffa`c9cd71ca : gl_wrapper!gl::GLApiBase::glDrawArraysFn+0x36 [j:\chromium_build\chromium\src\ui\gl\gl_bindings_autogen_gl.cc @ 3732]
0b 00007ffa`c9d4fcf7 : 00000273`ad1d1598 00007ffa`c9d95511 00000273`a4e7414c 00000273`a4e740d8 : gl_wrapper!gl::RealGLApi::glDrawArraysFn+0x49 [j:\chromium_build\chromium\src\ui\gl\gl_gl_api_implementation.cc @ 434]
0c 00007ffa`c9d84f0f : 00000273`ad1d1598 00000001`219fc9b0 00000273`ad1d1590 00000273`ad520350 : gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays+0x57 [j:\chromium_build\chromium\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc @ 1227]
0d 00007ffa`c9d1d1a6 : 0000a3f5`85e7346b 00007ffa`c9d277c0 00000000`00000003 0000008f`00000001 : gles2!gpu::gles2::GLES2DecoderPassthroughImpl::HandleDrawArrays+0x7f [j:\chromium_build\chromium\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_handlers.cc @ 124]
0e 00007ffa`c9d1c87d : 0000008f`219fcbe8 00007ffa`f914612f 00000273`ad520350 00000273`ad520388 :

gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>+0x286
[j:\chromium_build\chromium\src\gpu\command_buffer\service\gles2_cmd_decoder_passthr
ough.cc @ 835]
0f 00007ffa`f91817f1 : 0000a1a2`0713b2a8 00007ffa`f9137ba3 0000008f`219fcb00
0000008f`219fcbc8 :
gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands+0x9d
[j:\chromium_build\chromium\src\gpu\command_buffer\service\gles2_cmd_decoder_passthr
ough.cc @ 773]
10 00007ffa`c99051a6 : 0000008f`219fcd88 0000008f`219fd0f8 00000273`ad5b3f2c
0000008f`219fd0f8 : gpu!gpu::CommandBufferService::Flush+0x751
[j:\chromium_build\chromium\src\gpu\command_buffer\service\command_buffer_service.cc
@ 68]
11 00007ffa`c9911d3e : 0000008f`219fd1c8 00007ffa`f9281b66 0000008f`219fd1d0
0000008f`219fd1d0 : gpu_ipc_service!gpu::CommandBufferStub::OnAsyncFlush+0x766
[j:\chromium_build\chromium\src\gpu\ipc\service\command_buffer_stub.cc @ 518]
12 00007ffa`c9911c6b : 0000008f`219fd1d0 00007ffa`c9911a4b 00000273`ad3eb2c0
0000008f`219fd0f8 :
gpu_ipc_service!base::DispatchToMethodImpl<gpu::CommandBufferStub *,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > >,0,1,2>+0x9e
[j:\chromium_build\chromium\src\base\tuple.h @ 53]
13 00007ffa`c991195f : 0000008f`219fd1d0 0000008f`219fd1cc 0000008f`219fd1c8
0000008f`219fd1c8 : gpu_ipc_service!base::DispatchToMethod<gpu::CommandBufferStub
,void (gpu::CommandBufferStub::)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > > >+0x6b
[j:\chromium_build\chromium\src\base\tuple.h @ 60]
14 00007ffa`c99049ca : 00000000`00000000 0000008f`219fd3d0 00000000`00000000
0000008f`219fd3d0 :
gpu_ipc_service!IPC::DispatchToMethod<gpu::CommandBufferStub,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),void,std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > > >+0x5f
[j:\chromium_build\chromium\src\ipc\ipc_message_templates.h @ 52]
15 00007ffa`c9902840 : 0000008f`219fd278 0000008f`219fd318 0000008f`219fd318
0000008f`219fd3e8 :
gpu_ipc_service!IPC::MessageT<GpuCommandBufferMsg_AsyncFlush_Meta,std::__1::tupl
e<int,unsigned int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
>,void>::Dispatch<gpu::CommandBufferStub,gpu::CommandBufferStub,void,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > &)>+0x24a
[j:\chromium_build\chromium\src\ipc\ipc_message_templates.h @ 141]
*** WARNING: Unable to verify checksum for
J:\chromium_build\chromium\src\out\Default\ipc.dll

16 00007ffa`ff35b26a : 00000273`ad891e80 00007ffa`c9912bf6 00000273`a8e48d00 00000000`00000000 : gpu_ipc_service!gpu::CommandBufferStub::OnMessageReceived+0x750 [j:\chromium_build\chromium\src\gpu\ipc\service\command_buffer_stub.cc @ 166]
17 00007ffa`c992d6a9 : 00000273`ad88af20 00000000`00000000 00000fc5`86e02e26 00007ffa`c992add9 : ipc!IPC::MessageRouter::RouteMessage+0x7a [j:\chromium_build\chromium\src\ipc\message_router.cc @ 57]
18 00007ffa`c99288de : 0100008f`219fd5c8 0000008f`219fd5c8 0000008f`219fd5c8 00007ffb`06a9877d : gpu_ipc_service!gpu::GpuChannel::HandleMessageHelper+0x79 [j:\chromium_build\chromium\src\gpu\ipc\service\gpu_channel.cc @ 630]
19 00007ffa`c9937b39 : 0000008f`219fd7f8 00007ffa`f9141e97 00000273`a8e48cd0 00000273`ad3eb2b0 : gpu_ipc_service!gpu::GpuChannel::HandleMessage+0x21e [j:\chromium_build\chromium\src\gpu\ipc\service\gpu_channel.cc @ 591]
1a 00007ffa`c99379d4 : 00000273`ad3eb2b0 00007ffa`c9937cb3 00000273`ad847518 00007ffa`f9140bd9 : gpu_ipc_service!base::internal::FunctorTraits<void (gpu::GpuChannel::*)(const IPC::Message &),void>::Invoke<void (gpu::GpuChannel::*)(const IPC::Message &),base::WeakPtr<gpu::GpuChannel>,IPC::Message>+0x59 [j:\chromium_build\chromium\src\base\bind_internal.h @ 498]
1b 00007ffa`c993791d : 0000008f`00000001 00007ffa`f9153dfa 00000c18`00000001 0000008f`219fd898 : gpu_ipc_service!base::internal::InvokeHelper<1,void>::MakeItSo<void (gpu::GpuChannel::*)(const IPC::Message &),base::WeakPtr<gpu::GpuChannel>,IPC::Message>+0x84 [j:\chromium_build\chromium\src\base\bind_internal.h @ 660]
1c 00007ffa`c993789d : 0000008f`00000000 00007ffb`06ad9a18 0000a1a2`0713a338 00007ffa`f9153d33 : gpu_ipc_service!base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)(const IPC::Message &),base::WeakPtr<gpu::GpuChannel>,IPC::Message>,void ()>::RunImpl<void (gpu::GpuChannel::*)(const IPC::Message &),std::__1::tuple<base::WeakPtr<gpu::GpuChannel>,IPC::Message>,0,1>+0x6d [j:\chromium_build\chromium\src\base\bind_internal.h @ 710]
1d 00007ffa`f91992fc : 00000273`ad8474d0 00000c18`a4e740d8 00000273`a4e740d8 00000000`00000000 : gpu_ipc_service!base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)(const IPC::Message &),base::WeakPtr<gpu::GpuChannel>,IPC::Message>,void ()>::RunOnce+0x5d [j:\chromium_build\chromium\src\base\bind_internal.h @ 679]
1e 00007ffa`f9198a3b : 0000008f`219fd9c8 00007ffb`06904307 0000008f`00000000 00007ffb`06ad9a18 : gpu!base::OnceCallback<void ()>::Run+0x7c [j:\chromium_build\chromium\src\base\callback.h @ 100]
1f 00007ffa`f91ad66f : 00000273`ad9a0dd8 00007ffa`f91ab063 00000273`ad9a0dd8 00007ffa`f91ab363 : gpu!gpu::Scheduler::RunNextTask+0x92b [j:\chromium_build\chromium\src\gpu\command_buffer\service\scheduler.cc @ 562]
20 00007ffa`f91ad60b : 00000273`ad9a0dd8 00007ffa`f91ab01b 0000008f`219fdd78 0000008f`219fdd58 : gpu!base::internal::FunctorTraits<void (gpu::Scheduler::*)(),void>::Invoke<void (gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler>>+0x1f [j:\chromium_build\chromium\src\base\bind_internal.h @ 498]

21 00007ffa`f91ad599 : 0000008f`219fdd30 00007ffb`069064e7 0000008f`219fdd40 00007ffb`06be41d5 : gpu!base::internal::InvokeHelper<1,void>::MakeItSo<void (gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler>>+0x4b [j:\chromium_build\chromium\src\base\bind_internal.h @ 660]
22 00007ffa`f91ad53d : 00007ffb`06f22468 00007ffb`06f22468 00000fc5`86e02666 00007ffb`06906423 : gpu!base::internal::Invoker<base::internal::BindState<void (gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler> >,void ()>::RunImpl<void (gpu::Scheduler::*)(),std::__1::tuple<base::WeakPtr<gpu::Scheduler> >,0>+0x49 [j:\chromium_build\chromium\src\base\bind_internal.h @ 710]
23 00007ffb`0690208c : 00000003`219fdf90 00000273`a4dfa0e0 00000fc5`86e02666 00007ffb`06af9b20 : gpu!base::internal::Invoker<base::internal::BindState<void (gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler> >,void ()>::RunOnce+0x5d [j:\chromium_build\chromium\src\base\bind_internal.h @ 679]
24 00007ffb`06af961f : 00000273`a4e7a770 00007ffb`069042de 00000273`a4e7a768 00007ffb`06b162ea : base!base::OnceCallback<void ()>::Run+0x7c [j:\chromium_build\chromium\src\base\callback.h @ 100]
25 00007ffb`06b4cee2 : 00000000`00000000 00007ffb`06be41d5 00000000`00000000 0000008f`219fe068 : base!base::TaskAnnotator::RunTask+0x70f [j:\chromium_build\chromium\src\base\task\common\task_annotator.cc @ 144]
26 00007ffb`06b4c45e : 00000fc5`86e01846 00000000`00000000 00000000`0001df04 00000000`0001df04 : base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl+0x802 [j:\chromium_build\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 334]
27 00007ffb`069b84ae : 00000273`a89b18e0 0000008f`219fe4c8 00000273`a89b18e8 0000008f`219fe4c8 : base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork+0xfe [j:\chromium_build\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 255]
28 00007ffb`06b4df0f : 00000273`a8be0138 00007ffb`0697b3db 00000000`00000000 00000001`00000000 : base!base::MessagePumpDefault::Run+0xae [j:\chromium_build\chromium\src\base\message_loop\message_pump_default.cc @ 40]
29 00007ffb`06a7e822 : 00000000`00000000 00000000`000000e6 00000fc5`86e01c46 00007ffb`06ccc588 : base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0x36f [j:\chromium_build\chromium\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 456]
*** WARNING: Unable to verify checksum for J:\chromium_build\chromium\src\out\Default\content.dll
2a 00007ffa`f940d414 : 00000000`000003d8 00000000`00000600 00000000`00000000 0000008f`219fea00 : base!base::RunLoop::Run+0x342 [j:\chromium_build\chromium\src\base\run_loop.cc @ 124]
2b 00007ffa`fd64ee70 : 0000008f`219fede8 00000273`a4e27160 0000008f`219ff438 00000273`a4de4490 : content!content::GpuMain+0xaf4 [j:\chromium_build\chromium\src\content\gpu\gpu_main.cc @ 446]

2c 00007ffa`fd6501f7 : 0000008f`219fee70 00000000`00000000 00000000`00000000 00000000`00000000 : content!content::RunOtherNamedProcessTypeMain+0xe0 [j:\chromium_build\chromium\src\content\app\content_main_runner_impl.cc @ 547]
2d 00007ffa`fd64ab97 : 00000000`00000000 00000000`00000000 00000000`00000000 00000000`00000000 : content!content::ContentMainRunnerImpl::Run+0x2f7 [j:\chromium_build\chromium\src\content\app\content_main_runner_impl.cc @ 882]
*** WARNING: Unable to verify checksum for J:\chromium_build\chromium\src\out\Default\embedder.dll
2e 00007ffa`c7d12498 : 00000273`a4dd0000 00007ffb`7dabb997 00000273`a4d50000 00007ffb`00000000 : content!content::ContentServiceManagerMainDelegate::RunEmbedderProcess+0x37 [j:\chromium_build\chromium\src\content\app\content_service_manager_main_delegate.cc @ 60]
2f 00007ffa`fd64ec28 : 00007ffb`57be40bd 00000000`00000008 7373656c`64616568 00000000`00000000 : embedder!service_manager::Main+0x858 [j:\chromium_build\chromium\src\services\service_manager\embedder\main.cc @ 453]

Crash Information

3:033> !analyze -v
****
*   *
*   Exception Analysis   *
*   *
****

*** WARNING: Unable to verify checksum for J:\chromium_build\chromium\src\out\Default\mojo_core_embedder_internal.dll

KEY_VALUES_STRING: 1

    Key : AV.Fault
    Value: Read

    Key : Analysis.CPU.mSec
    Value: 7139

    Key : Analysis.DebugAnalysisProvider.CPP
    Value: Create: 8007007e on CLAB

    Key : Analysis.DebugData
    Value: CreateObject

    Key : Analysis.DebugModel
    Value: CreateObject

    Key : Analysis.Elapsed.mSec

Value: 158581

Key : Analysis.Memory.CommitPeak.Mb
Value: 3748

Key : Analysis.System
Value: CreateObject

Key : Timeline.OS.Boot.DeltaSec
Value: 21978

Key : Timeline.Process.Start.DeltaSec
Value: 348

Key : WER.OS.Branch
Value: 19h1_release

Key : WER.OS.Timestamp
Value: 2019-03-18T12:02:00Z

Key : WER.OS.Version
Value: 10.0.18362.1

Key : WER.Process.Version
Value: 86.0.4205.0

ADDITIONAL_XML: 1

OS_BUILD_LAYERS: 1

EXCEPTION_RECORD: (.exr -1)
ExceptionAddress: 00007ffabfe85a79
(libglesv2!rx::Buffer11::BufferStorage::getSize+0x0000000000000009)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 0000000000000000
   Parameter[1]: ffffffffffffffff
Attempt to read from address ffffffffffffffff

FAULTING_THREAD: 00003b9c

PROCESS_NAME: chrome.exe

READ_ADDRESS: ffffffffffffffff

ERROR_CODE: (NTSTATUS) 0xc0000005 - The instruction at 0x%p referenced memory at 0x%p. The memory could not be %s.

EXCEPTION_CODE_STR: c0000005

EXCEPTION_PARAMETER1: 0000000000000000

EXCEPTION_PARAMETER2: ffffffffffffffff

STACK_TEXT:
0000008f`219fb490 00007ffa`bfe88786   : 00000273`ad4c3be0 00000273`a8a0ba60
0000008f`219fb660 00007ffb`782dec50 : libglesv2!rx::Buffer11::BufferStorage::getSize+0x9
0000008f`219fb4a0 00007ffa`bfe8851a   : 00000000`ad6d1730 00007ffa`bf96c889
00000273`a8a0ba60 00000000`00008000 :
libglesv2!rx::Buffer11::getBufferStorage<rx::Buffer11::NativeStorage>+0x1f6
0000008f`219fb7a0 00007ffa`bff39609   : 00000273`a8d45888 0000008f`219fbda8
01000000`00000010 00007ffa`bf996d00 : libglesv2!rx::Buffer11::getBuffer+0x6a
0000008f`219fb820 00007ffa`bff32e43   : 0000008f`219fbf08 0000008f`219fbf08
0000008f`219fc338 00007ffa`bf96a39d :
libglesv2!rx::StateManager11::applyVertexBuffers+0x8b9
0000008f`219fbdd0 00007ffa`bff30dd6   : 00000273`a89ed8b0 00000273`ad953200
00000273`ad956010 00000000`00000000 :
libglesv2!rx::StateManager11::syncVertexBuffersAndInputLayout+0x433
0000008f`219fbf40 00007ffa`bfea121d   : 000040cb`d408ccef 00007ffa`bf7f800a
00007ffa`c0a04b10 00000273`ad956618 : libglesv2!rx::StateManager11::updateState+0xfd6
0000008f`219fc4b0 00007ffa`bf7e67f2   : 00000273`ad953200 00000010`01bff74c
0100008f`00000004 00007ffa`bf7e66f7 : libglesv2!rx::Context11::drawArrays+0x21d
0000008f`219fc6a0 00007ffa`bf7e6667   : 00000000`00000001 0000008f`219fc800
00007ffa`c0972971 00000000`00000008 : libglesv2!gl::Context::drawArrays+0xe2
0000008f`219fc710 00007ffa`bf8d95e3   : 00000273`ad5719d8 00000001`219fc908
00000001`00000001 00000001`00000004 : libglesv2!gl::DrawArrays+0x167
0000008f`219fc7b0 00007ffa`d1de5226   : 00000273`a8ea0f00 00000273`a8ea0f04
00000273`a8ea0dc0 00000273`a8ea0dc0 : libglesv2!glDrawArrays+0x23
0000008f`219fc7f0 00007ffa`d1e619f9   : 00000273`ad5221e0 00007ffa`c9d4fc32
00000273`ad1d1590 00007ffa`c9cd71ca : gl_wrapper!gl::GLApiBase::glDrawArraysFn+0x36
0000008f`219fc830 00007ffa`c9d4fcf7   : 00000273`ad1d1598 00007ffa`c9d95511
00000273`a4e7414c 00000273`a4e740d8 :
gl_wrapper!gl::RealGLApi::glDrawArraysFn+0x49
0000008f`219fc880 00007ffa`c9d84f0f   : 00000273`ad1d1598 00000001`219fc9b0
00000273`ad1d1590 00000273`ad520350 :
gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays+0x57
0000008f`219fc8d0 00007ffa`c9d1d1a6   : 0000a3f5`85e7346b 00007ffa`c9d277c0
00000000`00000003 0000008f`00000001 :
gles2!gpu::gles2::GLES2DecoderPassthroughImpl::HandleDrawArrays+0x7f
0000008f`219fc930 00007ffa`c9d1c87d   : 0000008f`219fcbe8 00007ffa`f914612f
00000273`ad520350 00000273`ad520388 :
gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>+0x286

0000008f`219fc9e0 00007ffa`f91817f1 : 0000a1a2`0713b2a8 00007ffa`f9137ba3
0000008f`219fcb00 0000008f`219fcbc8 :
gles2!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands+0x9d
0000008f`219fca50 00007ffa`c99051a6 : 0000008f`219fcd88 0000008f`219fd0f8
00000273`ad5b3f2c 0000008f`219fd0f8 : gpu!gpu::CommandBufferService::Flush+0x751
0000008f`219fcca0 00007ffa`c9911d3e : 0000008f`219fd1c8 00007ffa`f9281b66
0000008f`219fd1d0 0000008f`219fd1d0 :
gpu_ipc_service!gpu::CommandBufferStub::OnAsyncFlush+0x766
0000008f`219fcfd0 00007ffa`c9911c6b : 0000008f`219fd1d0 00007ffa`c9911a4b
00000273`ad3eb2c0 0000008f`219fd0f8 :
gpu_ipc_service!base::DispatchToMethodImpl<gpu::CommandBufferStub *,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > >,0,1,2>+0x9e
0000008f`219fd040 00007ffa`c991195f : 0000008f`219fd1d0 0000008f`219fd1cc
0000008f`219fd1c8 0000008f`219fd1c8 :
gpu_ipc_service!base::DispatchToMethod<gpu::CommandBufferStub *,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > > >+0x6b
0000008f`219fd0b0 00007ffa`c99049ca : 00000000`00000000 0000008f`219fd3d0
00000000`00000000 0000008f`219fd3d0 :
gpu_ipc_service!IPC::DispatchToMethod<gpu::CommandBufferStub,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
&),void,std::__1::tuple<int,unsigned
int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > > >+0x5f
0000008f`219fd120 00007ffa`c9902840 : 0000008f`219fd278 0000008f`219fd318
0000008f`219fd318 0000008f`219fd3e8 :
gpu_ipc_service!IPC::MessageT<GpuCommandBufferMsg_AsyncFlush_Meta,std::__1::tupl
e<int,unsigned int,std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> >
>,void>::Dispatch<gpu::CommandBufferStub,gpu::CommandBufferStub,void,void
(gpu::CommandBufferStub::*)(int, unsigned int, const
std::__1::vector<gpu::SyncToken,std::__1::allocator<gpu::SyncToken> > &)>+0x24a
0000008f`219fd220 00007ffa`ff35b26a : 00000273`ad891e80 00007ffa`c9912bf6
00000273`a8e48d00 00000000`00000000 :
gpu_ipc_service!gpu::CommandBufferStub::OnMessageReceived+0x750
0000008f`219fd4a0 00007ffa`c992d6a9 : 00000273`ad88af20 00000000`00000000
00000fc5`86e02e26 00007ffa`c992add9 : ipc!IPC::MessageRouter::RouteMessage+0x7a
0000008f`219fd500 00007ffa`c99288de : 0100008f`219fd5c8 0000008f`219fd5c8
0000008f`219fd5c8 00007ffb`06a9877d :
gpu_ipc_service!gpu::GpuChannel::HandleMessageHelper+0x79
0000008f`219fd550 00007ffa`c9937b39 : 0000008f`219fd7f8 00007ffa`f9141e97
00000273`a8e48cd0 00000273`ad3eb2b0 :
gpu_ipc_service!gpu::GpuChannel::HandleMessage+0x21e

0000008f`219fd790 00007ffa`c99379d4   : 00000273`ad3eb2b0 00007ffa`c9937cb3
00000273`ad847518 00007ffa`f9140bd9 :
gpu_ipc_service!base::internal::FunctorTraits<void (gpu::GpuChannel::*)(const
IPC::Message &),void>::Invoke<void (gpu::GpuChannel::*)(const IPC::Message
&),base::WeakPtr<gpu::GpuChannel>,IPC::Message>+0x59
0000008f`219fd7f0 00007ffa`c993791d   : 0000008f`00000001 00007ffa`f9153dfa
00000c18`00000001 0000008f`219fd898 :
gpu_ipc_service!base::internal::InvokeHelper<1,void>::MakeItSo<void
(gpu::GpuChannel::*)(const IPC::Message
&),base::WeakPtr<gpu::GpuChannel>,IPC::Message>+0x84
0000008f`219fd860 00007ffa`c993789d   : 0000008f`00000000 00007ffb`06ad9a18
0000a1a2`0713a338 00007ffa`f9153d33 :
gpu_ipc_service!base::internal::Invoker<base::internal::BindState<void
(gpu::GpuChannel::*)(const IPC::Message
&),base::WeakPtr<gpu::GpuChannel>,IPC::Message>,void ()>::RunImpl<void
(gpu::GpuChannel::*)(const IPC::Message
&),std::__1::tuple<base::WeakPtr<gpu::GpuChannel>,IPC::Message>,0,1>+0x6d
0000008f`219fd8b0 00007ffa`f91992fc   : 00000273`ad8474d0 00000c18`a4e740d8
00000273`a4e740d8 00000000`00000000 :
gpu_ipc_service!base::internal::Invoker<base::internal::BindState<void
(gpu::GpuChannel::*)(const IPC::Message
&),base::WeakPtr<gpu::GpuChannel>,IPC::Message>,void ()>::RunOnce+0x5d
0000008f`219fd900 00007ffa`f9198a3b   : 0000008f`219fd9c8 00007ffb`06904307
0000008f`00000000 00007ffb`06ad9a18 : gpu!base::OnceCallback<void ()>::Run+0x7c
0000008f`219fd960 00007ffa`f91ad66f   : 00000273`ad9a0dd8 00007ffa`f91ab063
00000273`ad9a0dd8 00007ffa`f91ab363 : gpu!gpu::Scheduler::RunNextTask+0x92b
0000008f`219fdc40 00007ffa`f91ad60b   : 00000273`ad9a0dd8 00007ffa`f91ab01b
0000008f`219fdd78 0000008f`219fdd58 : gpu!base::internal::FunctorTraits<void
(gpu::Scheduler::*)(),void>::Invoke<void
(gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler>>+0x1f
0000008f`219fdc80 00007ffa`f91ad599   : 0000008f`219fdd30 00007ffb`069064e7
0000008f`219fdd40 00007ffb`06be41d5 :
gpu!base::internal::InvokeHelper<1,void>::MakeItSo<void
(gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler>>+0x4b
0000008f`219fdcc0 00007ffa`f91ad53d   : 00007ffb`06f22468 00007ffb`06f22468
00000fc5`86e02666 00007ffb`06906423 :
gpu!base::internal::Invoker<base::internal::BindState<void
(gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler> >,void ()>::RunImpl<void
(gpu::Scheduler::*)(),std::__1::tuple<base::WeakPtr<gpu::Scheduler> >,0>+0x49
0000008f`219fdd10 00007ffb`0690208c   : 00000003`219fdf90 00000273`a4dfa0e0
00000fc5`86e02666 00007ffb`06af9b20 :
gpu!base::internal::Invoker<base::internal::BindState<void
(gpu::Scheduler::*)(),base::WeakPtr<gpu::Scheduler> >,void ()>::RunOnce+0x5d
0000008f`219fdd60 00007ffb`06af961f   : 00000273`a4e7a770 00007ffb`069042de
00000273`a4e7a768 00007ffb`06b162ea : base!base::OnceCallback<void ()>::Run+0x7c
0000008f`219fddc0 00007ffb`06b4cee2   : 00000000`00000000 00007ffb`06be41d5
00000000`00000000 0000008f`219fe068 : base!base::TaskAnnotator::RunTask+0x70f

0000008f`219fdfd0 00007ffb`06b4c45e : 00000fc5`86e01846 00000000`00000000
00000000`0001df04 00000000`0001df04 :
base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkI
mpl+0x802
0000008f`219fe350 00007ffb`069b84ae : 00000273`a89b18e0 0000008f`219fe4c8
00000273`a89b18e8 0000008f`219fe4c8 :
base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
+0xfe
0000008f`219fe440 00007ffb`06b4df0f : 00000273`a8be0138 00007ffb`0697b3db
00000000`00000000 00000001`00000000 : base!base::MessagePumpDefault::Run+0xae
0000008f`219fe4e0 00007ffb`06a7e822 : 00000000`00000000 00000000`000000e6
00000fc5`86e01c46 00007ffb`06ccc588 :
base!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0x
36f
0000008f`219fe730 00007ffa`f940d414 : 00000000`000003d8 00000000`00000600
00000000`00000000 0000008f`219fea00 : base!base::RunLoop::Run+0x342
0000008f`219fe870 00007ffa`fd64ee70 : 0000008f`219fede8 00000273`a4e27160
0000008f`219ff438 00000273`a4de4490 : content!content::GpuMain+0xaf4
0000008f`219fedb0 00007ffa`fd6501f7 : 0000008f`219fee70 00000000`00000000
00000000`00000000 00000000`00000000 :
content!content::RunOtherNamedProcessTypeMain+0xe0
0000008f`219fee20 00007ffa`fd64ab97 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 :
content!content::ContentMainRunnerImpl::Run+0x2f7
0000008f`219fef20 00007ffa`c7d12498 : 00000273`a4dd0000 00007ffb`7dabb997
00000273`a4d50000 00007ffb`00000000 :
content!content::ContentServiceManagerMainDelegate::RunEmbedderProcess+0x37
0000008f`219fef60 00007ffa`fd64ec28 : 00007ffb`57be40bd 00000000`00000008
7373656c`64616568 00000000`00000000 : embedder!service_manager::Main+0x858
0000008f`219ff2a0 00007ffa`ebaf139f : 0000008f`219ff488 00007ff6`029f5b55
00000000`00000000 00000000`219ff488 : content!content::ContentMain+0x88
0000008f`219ff350 00007ff6`029f5ba5 : 00000000`00000000 00007ffa`ebaf1140
00000000`00000000 00000000`00000000 : chrome!ChromeMain+0x25f
0000008f`219ff4b0 00007ff6`029f1806 : 00007ffb`0612e0b0 00007ffb`061175a0
00007ffb`061175e0 00007ffb`06117870 : chrome_exe!MainDllLoader::Launch+0x2d5
0000008f`219ff5c0 00007ff6`02cb51f2 : 00000000`00000000 00007ff6`02cb2dbd
00000000`00000000 00007ff6`02cf45d8 : chrome_exe!wWinMain+0x806
0000008f`219ff9b0 00007ff6`02cb532e : 00007ff6`02cf4500 00007ff6`02cf45b0
00000000`00000000 00000000`00000000 : chrome_exe!invoke_main+0x32
0000008f`219ff9f0 00007ff6`02cb53ae : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : chrome_exe!__scrt_common_main_seh+0x12e
0000008f`219ffa60 00007ff6`02cb53c9 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : chrome_exe!__scrt_common_main+0xe
0000008f`219ffa90 00007ffb`7bf57bd4 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : chrome_exe!wWinMainCRTStartup+0x9
0000008f`219ffac0 00007ffb`7daece51 : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : KERNEL32!BaseThreadInitThunk+0x14

0000008f`219ffaf0 00000000`00000000   : 00000000`00000000 00000000`00000000
00000000`00000000 00000000`00000000 : ntdll!RtlUserThreadStart+0x21

FAULTING_SOURCE_LINE:
j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer11.cpp

FAULTING_SOURCE_FILE:
j:\chromium_build\chromium\src\third_party\angle\src\libANGLE\renderer\d3d\d3d11\Buffer11.cpp

FAULTING_SOURCE_LINE_NUMBER: 115

FAULTING_SOURCE_CODE:
```
   111:     virtual ~BufferStorage() {}
   112:
   113:     DataRevision getDataRevision() const { return mRevision; }
   114:     BufferUsage getUsage() const { return mUsage; }
>  115:     size_t getSize() const { return mBufferSize; }
   116:     void setDataRevision(DataRevision rev) { mRevision = rev; }
   117:
   118:     virtual bool isCPUAccessible(GLbitfield access) const = 0;
   119:
   120:     virtual bool isGPUAccessible() const = 0;
```

SYMBOL_NAME: libglesv2!rx::Buffer11::BufferStorage::getSize+9

MODULE_NAME: libglesv2

IMAGE_NAME: libglesv2.dll

STACK_COMMAND: ~33s ; .cxr ; kb

FAILURE_BUCKET_ID:
INVALID_POINTER_READ_c0000005_libglesv2.dll!rx::Buffer11::BufferStorage::getSize

OS_VERSION: 10.0.18362.1

BUILDLAB_STR: 19h1_release

OSPLATFORM_TYPE: x64

OSNAME: Windows 10

IMAGE_VERSION: 2.1.0.0

FAILURE_ID_HASH: {c4781cef-0e7c-635c-0739-b61f18ddcde6}

Followup: MachineOwner

Timeline

2020-07-20 - Vendor Disclosure

2020-07-30 - Vendor patched

2020-10-20 - Public Release

Credit

Discovered by Piotr Bania of Cisco Talos.