Starred by 4 users

Owner:	jmad...@chromium.org
CC:	w...@chromium.org jmad...@chromium.org
Status:	Verified *(Closed)*
Components:	Internals>GPU>ANGLE
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Severity-High
allpublic
reward-inprocess
ClusterFuzz-Verified
Test-Predator-Auto-Components
Test-Predator-Auto-Owner
CVE_description-submitted
external_security_report
M-98
reward-7000
Target-98
FoundIn-96
FoundIn-97
FoundIn-100
Security_Impact-Extended
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0975

Issue 1295411: Security: [ANGLE] Heap use-after-free in CommandBufferHelperCommon::bufferWrite

Reported by ggabu...@gmail.com on Tue, Feb 8, 2022, 2:53 PM EST

Code

VULNERABILITY DETAILS

There is a heap use-after-free vulnerability in Vulkan backend that could be triggered in Swiftshader.
I think that this vulnerability started in commit 8270ebbd627d24eb87c61fde1282f52a6e085653.

VERSION

Chrome Version: master (and tested on 98.0.4758.82 (Official Build) (64-bit) Stable)
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:

```
=================================================================
==8856==ERROR: AddressSanitizer: heap-use-after-free on address 0x121f83da60b0 at pc 0x7ffce1d2f418 bp
0x00ea733fdf40 sp 0x00ea733fdf88
READ of size 8 at 0x121f83da60b0 thread T0
==8856==WARNING: Failed to use and restart external symbolizer!
==8856==*** WARNING: Failed to initialize DbgHelp!              ***
==8856==*** Most likely this means that the app is already      ***
==8856==*** using DbgHelp, possibly with incompatible flags.    ***
==8856==*** Due to technical reasons, symbolization might crash ***
==8856==*** or produce wrong results.                           ***
    #0 0x7ffce1d2f417 in rx::vk::CommandBufferHelperCommon::bufferWrite
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:1079
    #1 0x7ffce1bc7bb3 in rx::ContextVk::handleDirtyGraphicsTransformFeedbackBuffersEmulation
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:2069
    #2 0x7ffce1bce874 in rx::ContextVk::setupDraw
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:1188
    #3 0x7ffce1bd8db9 in rx::ContextVk::drawArrays

C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:2738
    #4 0x7ffce1471f71 in GL_DrawArrays
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:1100
```

C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:1109
    #5 0x7ffca4328952 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDrawArrays
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:1217
    #6 0x7ffca07ac7ad in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:871
    #7 0x7ffca07abbf4 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:809
    #8 0x7ffc9d6c81e0 in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #9 0x7ffc9aba44e8 in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:499
    #10 0x7ffc9aba36c2 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:151
    #11 0x7ffc9abaffbb in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:669
    #12 0x7ffc9abbade1 in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
    #13 0x7ffc9a7d4f30 in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:684
    #14 0x7ffc99410274 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
    #15 0x7ffc9c0d25c5 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:387
    #16 0x7ffc9c0d1b99 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:292
    #17 0x7ffc9c0aa317 in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:38
    #18 0x7ffc9c0d3cf1 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:499
    #19 0x7ffc99390013 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
    #20 0x7ffc9bad4034 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:404
    #21 0x7ffc94eb598b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:683
    #22 0x7ffc94eb76af in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1043
    #23 0x7ffc94eb3fc6 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:399
    #24 0x7ffc94eb474a in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:427
    #25 0x7ffc8e60148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176
    #26 0x7ff79f1f5b16 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:167
    #27 0x7ff79f1f2b5f in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #28 0x7ff79f5f445f in __scrt_common_main_seh
d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #29 0x7ffd1f227033 in BaseThreadInitThunk+0x13 (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #30 0x7ffd1f362650 in RtlUserThreadStart+0x20 (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x121f83da60b0 is located 112 bytes inside of 320-byte region [0x121f83da6040,0x121f83da6180)
freed by thread T0 here:
    #0 0x7ff79f2a263b in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
    #1 0x7ffce1babc07 in rx::BufferVk::~BufferVk
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\BufferVk.cpp:257

    #2 0x7ffce14bfaaa in gl::Buffer::~Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:55
    #3 0x7ffce14c148b in gl::Buffer::~Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:54
    #4 0x7ffce1615143 in gl::TypedResourceManager<gl::Sampler,gl::SamplerManager,gl::SamplerID>::deleteObject

#4 0x7ffce1615143 in gl::TypedResourceManager<gl::Sampler,gl::SamplerManager,gl::SamplerID>::deleteObject
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:96
#5 0x7ffce151315b in gl::Context::deleteBuffers
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp:6712
#6 0x7ffce1470cb6 in GL_DeleteBuffers
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:819
#7 0x7ffca4325b75 in gpu::gles2::GLES2DecoderPassthroughImpl::DoDeleteBuffers
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:1012
#8 0x7ffca07ac7ad in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:871
#9 0x7ffca07abbf4 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:809
#10 0x7ffc9d6c81e0 in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
#11 0x7ffc9aba44e8 in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:499
#12 0x7ffc9aba36c2 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:151
#13 0x7ffc9abaffbb in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:669
#14 0x7ffc9abbade1 in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
#15 0x7ffc9a7d4f30 in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:684
#16 0x7ffc99410274 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
#17 0x7ffc9c0d25c5 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:387
#18 0x7ffc9c0d1b99 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:292
#19 0x7ffc9c0aa317 in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:38
#20 0x7ffc9c0d3cf1 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:499
#21 0x7ffc99390013 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
#22 0x7ffc9bad4034 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:404
#23 0x7ffc94eb598b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:683
#24 0x7ffc94eb76af in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1043
#25 0x7ffc94eb3fc6 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:399
#26 0x7ffc94eb474a in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:427
#27 0x7ffc8e60148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176

previously allocated by thread T0 here:
#0 0x7ff79f2a273b in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
#1 0x7ffce215f0a2 in operator new d:\A01_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
#2 0x7ffce1bea017 in rx::ContextVk::createBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\ContextVk.cpp:4470
#3 0x7ffce14bf812 in gl::Buffer::Buffer C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Buffer.cpp:47

#4 0x7ffce1616aad in gl::BufferManager::AllocateNewObject
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.cpp:114
#5 0x7ffce147c027 in gl::TypedResourceManager<gl::Buffer,gl::BufferManager,gl::BufferID>::checkObjectAllocationImpl<>

```
    #5 0x7ffce147c037 in gl::TypedResourceManager<gl::Buffer,gl::BufferManager,gl::BufferID>::checkObjectAllocationImpl<>
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\ResourceManager.h:117
    #6 0x7ffce146df00 in GL_BindBuffer
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_2_0_autogen.cpp:118
    #7 0x7ffca43208b7 in gpu::gles2::GLES2DecoderPassthroughImpl::DoBindBuffer
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc:390
    #8 0x7ffca07ac7ad in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl<0>
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:871
    #9 0x7ffca07abbf4 in gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc:809
    #10 0x7ffc9d6c81e0 in gpu::CommandBufferService::Flush
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc:70
    #11 0x7ffc9aba44e8 in gpu::CommandBufferStub::OnAsyncFlush
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:499
    #12 0x7ffc9aba36c2 in gpu::CommandBufferStub::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc:151
    #13 0x7ffc9abaffbb in gpu::GpuChannel::ExecuteDeferredRequest
C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc:669
    #14 0x7ffc9abbade1 in base::internal::Invoker<base::internal::BindState<void (gpu::GpuChannel::*)
(mojo::StructPtr<gpu::mojom::DeferredRequestParams>),base::WeakPtr<gpu::GpuChannel>,mojo::StructPtr<gpu::mojom::D
eferredRequestParams> >,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:748
    #15 0x7ffc9a7d4f30 in gpu::Scheduler::RunNextTask
C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc:684
    #16 0x7ffc99410274 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
    #17 0x7ffc9c0d25c5 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:387
    #18 0x7ffc9c0d1b99 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:292
    #19 0x7ffc9c0aa317 in base::MessagePumpDefault::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc:38
    #20 0x7ffc9c0d3cf1 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:499
    #21 0x7ffc99390013 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:141
    #22 0x7ffc9bad4034 in content::GpuMain C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc:404
    #23 0x7ffc94eb598b in content::RunOtherNamedProcessTypeMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:683
    #24 0x7ffc94eb76af in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1043
    #25 0x7ffc94eb3fc6 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:399
    #26 0x7ffc94eb474a in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:427
    #27 0x7ffc8e60148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:176

SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.cpp:1079 in
rx::vk::CommandBufferHelperCommon::bufferWrite
Shadow bytes around the buggy address:
  0x043f74534bc0: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x043f74534bd0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x043f74534be0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x043f74534bf0: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa

  0x043f74534c00: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
=>0x043f74534c10: fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd
  0x043f74534c20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

0x043f74534c20: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x043f74534c30: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
0x043f74534c40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x043f74534c50: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
0x043f74534c60: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
==8856==ABORTING
[6492:4828:0209/045110.685:ERROR:gpu_process_host.cc(974)] GPU process exited unexpectedly: exit_code=1

CREDIT INFORMATION
Reporter credit: SeongHwan Park (SeHwa)

poc.html
1.7 KB View Download

Comment 1 by sheriffbot on Tue, Feb 8, 2022, 2:54 PM EST Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Tue, Feb 8, 2022, 4:27 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=4852180762558464.

Comment 3 by ClusterFuzz on Tue, Feb 8, 2022, 5:23 PM EST Project Member

Labels: OS-Mac OS-Linux

Comment 4 by adetaylor@google.com on Tue, Feb 8, 2022, 5:49 PM EST Project Member

Cc: jmad...@chromium.org

ClusterFuzz has reproduced the UaF, but claims it is a duplicate of testcase 5315810746499072 (bug 1252274). They don't

appear similar to me so I have removed the duplicate status.

CF has not yet bisected, but cc jmadill@ since there seems to be a real issue here. After CF has finished its cogitations, it and I will label this issue all up appropriately.

Comment 5 by ClusterFuzz on Tue, Feb 8, 2022, 8:37 PM EST Project Member

Labels: OS-Android

Comment 6 by ClusterFuzz on Tue, Feb 8, 2022, 8:54 PM EST Project Member

Labels: OS-Windows

Comment 7 by ClusterFuzz on Wed, Feb 9, 2022, 7:50 AM EST Project Member

Labels: FoundIn-100 FoundIn-96 Security_Impact-Extended FoundIn-97

Detailed Report: https://clusterfuzz.com/testcase?key=4852180762558464

Fuzzer: None
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: GPU failure
Crash Address:
Crash State:
NULL
Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=861563:861564

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=4852180762558464

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 8 by ClusterFuzz on Wed, Feb 9, 2022, 8:19 AM EST Project Member

Labels: Test-Predator-Auto-Components
Components: Internals>GPU>ANGLE

Automatically applying components based on crash stacktrace and information from OWNERS files.

If this is incorrect, please apply the Test-Predator-Wrong-Components label.

Comment 9 by ClusterFuzz on Wed, Feb 9, 2022, 8:19 AM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: w...@chromium.org

Labels: Test-Predator-Auto-Owner

Automatically assigning owner based on suspected regression changelist https://chromium.googlesource.com/chromium/src/+/f7a9397ab90a433cd0403512e31edee2f4afb349 ([gpu] Log reasons for GPU process failure more clearly.).

If this is incorrect, please let us know why and apply the Test-Predator-Wrong-CLs label. If you aren't the correct owner for this issue, please unassign yourself as soon as possible so it can be re-triaged.

Comment 10 by adetaylor@google.com on Wed, Feb 9, 2022, 9:07 AM EST Project Member

Owner: jmad...@chromium.org
Cc: w...@chromium.org
Labels: Security_Severity-High Pri-1

I suspect Wez's CL is just changing the symptoms of the crash, rather than actually introducing it - so jmadill@ would you take care of it from here?

Rating as High as a UaF in a sandboxed process.

Comment 11 by sheriffbot on Wed, Feb 9, 2022, 12:47 PM EST Project Member

Labels: M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 12 by sheriffbot on Thu, Feb 24, 2022, 12:21 PM EST Project Member

jmadill: Uh oh! This issue still open and hasn't been updated in the last 15 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 13 by jmad...@chromium.org on Tue, Mar 1, 2022, 3:44 PM EST Project Member

Labels: -OS-Android

Comment 14 by Git Watcher on Fri, Mar 4, 2022, 8:05 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1

commit d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 21:14:47 2022

Protect against deleting a current XFB buffer.

~~Bug: chromium:1295411~~
Change-Id: I097f272c38e444e0af71aa55c0dc508a07aa0bd3
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498262
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1/src/libANGLE/validationES.h
[modify] https://crrev.com/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1/src/libANGLE/State.cpp
[modify] https://crrev.com/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1/src/libANGLE/validationES.cpp
[modify] https://crrev.com/d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1/src/libANGLE/validationES3.cpp

Comment 15 by Git Watcher on Fri, Mar 4, 2022, 9:35 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/91d805fceaf561052f3c943ff7f51fc057639138

commit 91d805fceaf561052f3c943ff7f51fc057639138
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Fri Mar 04 14:34:30 2022

Roll ANGLE from 75422a63785d to d9002eef2a5f (2 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/75422a63785d..d9002eef2a5f

2022-03-04 jmadill@chromium.org Protect against deleting a current XFB buffer.
2022-03-04 angle-autoroll@skia-public.iam.gserviceaccount.com Roll SwiftShader from 7089ef18891d to 561264b73b36 (7 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 romanl@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:1295411~~
Tbr: romanl@google.com

Change-Id: I628b83928f1c9ad884484908bcaa795414547c2e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3503524
Commit-Queue: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>

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@{#977642}

[modify] https://crrev.com/91d805fceaf561052f3c943ff7f51fc057639138/DEPS

Comment 16 by jmad...@chromium.org on Fri, Mar 4, 2022, 9:41 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 17 by sheriffbot on Fri, Mar 4, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Fri, Mar 4, 2022, 1:41 PM EST Project Member

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

Comment 19 by sheriffbot on Fri, Mar 4, 2022, 2:02 PM EST Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (977642) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (977642) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (977642) appears to be after beta branch point (972766).

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

Comment 20 by sheriffbot on Fri, Mar 4, 2022, 2:03 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?
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 21 by sheriffbot on Fri, Mar 4, 2022, 2:03 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 22 by sheriffbot on Fri, Mar 4, 2022, 2:03 PM EST Project Member

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

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

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

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

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

Comment 23 by ClusterFuzz on Mon, Mar 7, 2022, 5:19 AM EST Project Member

Status: Verified (was: Fixed)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 4852180762558464 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=977641:977643

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 24 by jmad...@chromium.org on Mon, Mar 7, 2022, 12:33 PM EST Project Member

1. use-after-free

2. https://chromium-review.googlesource.com/c/angle/angle/+/3498262
3. yes
4. no

Comment 25 by srinivassista@google.com on Mon, Mar 7, 2022, 12:37 PM EST Project Member

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

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

Comment 26 by srinivassista@google.com on Mon, Mar 7, 2022, 2:55 PM EST Project Member

This bug is approved for M100 merge, please complete your merge asap so this can be included in the beta release this week. Beta RC will be cut tomorrow (tuesday) March 8th at 3pm PST [Bulk Update]

Comment 27 by Git Watcher on Tue, Mar 8, 2022, 9:55 AM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f

commit 53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 21:14:47 2022

[M100] Protect against deleting a current XFB buffer.

~~Bug: chromium:1295411~~
Change-Id: I097f272c38e444e0af71aa55c0dc508a07aa0bd3
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498262
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3508698
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f/src/libANGLE/validationES.h
[modify] https://crrev.com/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f/src/libANGLE/State.cpp
[modify] https://crrev.com/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f/src/libANGLE/validationES.cpp
[modify] https://crrev.com/53c8915b5e7ac03ed1c0a7757c928ffe5e63a03f/src/libANGLE/validationES3.cpp

Comment 28 by amyressler@chromium.org on Tue, Mar 8, 2022, 6:20 PM EST Project Member

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

M99 merge approved, please merge to branch 4844 by noon PST, Thursday 10 March so this fix can be included in the next stable security refresh
M98 merge approved, please merge to branch 4758 so this fix can be included in Extended stable

Comment 29 by Git Watcher on Wed, Mar 9, 2022, 11:10 AM EST Project Member

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

The following revision refers to this bug:

https://chromium.googlesource.com/angle/angle/+/a62d5dbd5695272c8370c9cc9ded0108855c6af5

commit a62d5dbd5695272c8370c9cc9ded0108855c6af5
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 21:14:47 2022

[M99] Protect against deleting a current XFB buffer.

~~Bug: chromium:1295411~~
Change-Id: I097f272c38e444e0af71aa55c0dc508a07aa0bd3
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498262
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3514174
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/a62d5dbd5695272c8370c9cc9ded0108855c6af5/src/libANGLE/validationES.h
[modify] https://crrev.com/a62d5dbd5695272c8370c9cc9ded0108855c6af5/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/a62d5dbd5695272c8370c9cc9ded0108855c6af5/src/libANGLE/State.cpp
[modify] https://crrev.com/a62d5dbd5695272c8370c9cc9ded0108855c6af5/src/libANGLE/validationES3.cpp
[modify] https://crrev.com/a62d5dbd5695272c8370c9cc9ded0108855c6af5/src/libANGLE/validationES.cpp

Comment 30 by Git Watcher on Wed, Mar 9, 2022, 11:19 AM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/161f0866e8b8128c3df834e859195335ce2d126a

commit 161f0866e8b8128c3df834e859195335ce2d126a
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 21:14:47 2022

[M98] Protect against deleting a current XFB buffer.

~~Bug: chromium:1295411~~
Change-Id: I097f272c38e444e0af71aa55c0dc508a07aa0bd3
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498262
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit d9002eef2a5f27fc5d6b65d01d02afcfb9a35db1)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3514175
Reviewed-by: Ian Elliott <ianelliott@google.com>

[modify] https://crrev.com/161f0866e8b8128c3df834e859195335ce2d126a/src/libANGLE/validationES.h
[modify] https://crrev.com/161f0866e8b8128c3df834e859195335ce2d126a/src/libANGLE/State.cpp
[modify] https://crrev.com/161f0866e8b8128c3df834e859195335ce2d126a/src/libANGLE/validationES3.cpp
[modify] https://crrev.com/161f0866e8b8128c3df834e859195335ce2d126a/src/libANGLE/validationES.cpp

Comment 31 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 PM EST Project Member

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

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 32 by amyressler@chromium.org on Thu, Mar 10, 2022, 10:54 PM EST Project Member

Congratulations -- the VRP Panel has decided to award you $7,000 for this report. Thank you for reporting this issue to us and great work!

Comment 33 by amyressler@google.com on Fri, Mar 11, 2022, 2:50 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 34 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:27 PM EST Project Member

Labels: Release-1-M99

Comment 35 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0975 CVE_description-missing

Comment 36 by sheriffbot on Fri, Jun 10, 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

Comment 37 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 38 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:15 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing