Starred by 2 users

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

Hotlist-Merge-Review
Security_Severity-High
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
external_security_report
M-98
reward-7000
Target-98
FoundIn-98
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
LTS-Merge-Merged-96
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0976

Issue 1296866: Security: heap-buffer-overflow in getImageActualFormat

Reported by om...@krashconsulting.com on Sat, Feb 12, 2022, 4:31 PM EST

Code

Tested on Windows Chrome Dev 100.0.4878.0
and asan-linux-release-966194
with flags --no-sandbox --disable-gpu

```
3:046> r
rax=abababababababab rbx=0000000000000000 rcx=000001eeee1f1130
rdx=000001eeee1e7760 rsi=0000000000000001 rdi=000001eeee1f3e20
rip=00007ffb743559b4 rsp=000000e80adfdaa8 rbp=0000000000000000
 r8=0000000000000008  r9=0000000000000000 r10=0000000000000001
r11=0000000000000008 r12=0000000000000000 r13=0000000000000000
r14=000001eeee1f1130 r15=0000000000000000
iopl=0         nv up ei pl nz na po nc
cs=0033  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010206
libglesv2!rx::vk::ImageHelper::getActualFormat [inlined in libglesv2!rx::RenderTargetVk::getImageActualFormat+0x4]:
00007ffb`743559b4 48638004010000  movsxd  rax,dword ptr [rax+104h] ds:abababab`ababacaf=????????
3:046> k
 # Child-SP          RetAddr               Call Site
00 (Inline Function) --------`--------     libglesv2!rx::vk::ImageHelper::getActualFormat
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\vk_helpers.h @ 1659]
01 000000e8`0adfdaa8 00007ffb`743456d8     libglesv2!rx::RenderTargetVk::getImageActualFormat+0x4
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\RenderTargetVk.cpp @ 255]
02 000000e8`0adfdab0 00007ffb`74345ba7     libglesv2!rx::FramebufferVk::updateColorAttachment+0x58
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\FramebufferVk.cpp @ 1651]
03 000000e8`0adfdb20 00007ffb`7409e637     libglesv2!rx::FramebufferVk::syncState+0x197
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\renderer\vulkan\FramebufferVk.cpp @ 1866]
04 000000e8`0adfdd30 00007ffb`7407a404     libglesv2!gl::Framebuffer::syncState+0x47
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Framebuffer.cpp @ 2061]
05 (Inline Function) --------`--------     libglesv2!gl::State::syncDirtyObjects+0x37
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\State.h @ 1178]
06 (Inline Function) --------`--------     libglesv2!gl::Context::syncDirtyObjects+0x44
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.inl.h @ 107]
07 (Inline Function) --------`--------     libglesv2!gl::Context::prepareForCopyImage+0x44
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp @ 4201]
08 000000e8`0adfdd70 00007ffb`7403c57f     libglesv2!gl::Context::copyTexSubImage3D+0x84
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libANGLE\Context.cpp @ 4616]
09 000000e8`0adfde30 00007ffb`40331205     libglesv2!GL_CopyTexSubImage3D+0x12f
[C:\b\s\w\ir\cache\builder\src\third_party\angle\src\libGLESv2\entry_points_gles_3_0_autogen.cpp @ 524]
0a 000000e8`0adfdee0 00007ffb`416ba04c     chrome!gl::GLApiBase::glCopyTexSubImage3DFn+0x65
[C:\b\s\w\ir\cache\builder\src\ui\gl\gl_bindings_autogen_gl.cc @ 3549]
0b 000000e8`0adfdf50 00007ffb`416c5ede
chrome!gpu::gles2::GLES2DecoderPassthroughImpl::DoCopyTexSubImage3D+0x6c
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_doers.cc @ 955]
0c 000000e8`0adfdfd0 00007ffb`3a8f31eb

chrome!gpu::gles2::GLES2DecoderPassthroughImpl::HandleCopyTexSubImage3D+0x5e
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough_handlers_autogen.cc @ 547]
0d (Inline Function) --------`--------     chrome!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl+0xe4
```

0d (Inline Function) -------- -------- chrome!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommandsImpl+0xe4
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc @ 871]
0e 000000e8`0adfe040 00007ffb`39f24483 chrome!gpu::gles2::GLES2DecoderPassthroughImpl::DoCommands+0x10b
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\gles2_cmd_decoder_passthrough.cc @ 809]
0f 000000e8`0adfe0b0 00007ffb`39f238a9 chrome!gpu::CommandBufferService::Flush+0xf3
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\command_buffer_service.cc @ 73]
10 (Inline Function) --------`-------- chrome!gpu::CommandBufferStub::OnAsyncFlush+0xb3
[C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc @ 499]
11 000000e8`0adfe1c0 00007ffb`39f23528 chrome!gpu::CommandBufferStub::ExecuteDeferredRequest+0x159
[C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\command_buffer_stub.cc @ 151]
12 000000e8`0adfe300 00007ffb`3b986080 chrome!gpu::GpuChannel::ExecuteDeferredRequest+0xd8
[C:\b\s\w\ir\cache\builder\src\gpu\ipc\service\gpu_channel.cc @ 672]
13 (Inline Function) --------`-------- chrome!base::internal::FunctorTraits<void (policy::ManagementService::*)
(base::OnceCallback<void (policy::ManagementAuthorityTrustworthiness,
policy::ManagementAuthorityTrustworthiness)>),void>::Invoke+0x2d [C:\b\s\w\ir\cache\builder\src\base\bind_internal.h @
542]
14 (Inline Function) --------`-------- chrome!base::internal::InvokeHelper<1,void>::MakeItSo+0x44
[C:\b\s\w\ir\cache\builder\src\base\bind_internal.h @ 726]
15 (Inline Function) --------`-------- chrome!base::internal::Invoker<base::internal::BindState<void
(policy::ManagementService::*)(base::OnceCallback<void (policy::ManagementAuthorityTrustworthiness,
policy::ManagementAuthorityTrustworthiness)>),base::WeakPtr<policy::ManagementService>,base::OnceCallback<void
(policy::ManagementAuthorityTrustworthiness, policy::ManagementAuthorityTrustworthiness)> >,void ()>::RunImpl+0x44
[C:\b\s\w\ir\cache\builder\src\base\bind_internal.h @ 779]
16 000000e8`0adfe3a0 00007ffb`3a0c123a chrome!base::internal::Invoker<base::internal::BindState<void
(policy::ManagementService::*)(base::OnceCallback<void (policy::ManagementAuthorityTrustworthiness,
policy::ManagementAuthorityTrustworthiness)>),base::WeakPtr<policy::ManagementService>,base::OnceCallback<void
(policy::ManagementAuthorityTrustworthiness, policy::ManagementAuthorityTrustworthiness)> >,void ()>::RunOnce+0x60
[C:\b\s\w\ir\cache\builder\src\base\bind_internal.h @ 752]
17 (Inline Function) --------`-------- chrome!base::OnceCallback<void ()>::Run+0xd
[C:\b\s\w\ir\cache\builder\src\base\callback.h @ 142]
18 000000e8`0adfe3f0 00007ffb`3cc94720 chrome!gpu::Scheduler::RunNextTask+0x71a
[C:\b\s\w\ir\cache\builder\src\gpu\command_buffer\service\scheduler.cc @ 684]
19 (Inline Function) --------`-------- chrome!base::OnceCallback<void ()>::Run+0x17
[C:\b\s\w\ir\cache\builder\src\base\callback.h @ 142]
1a 000000e8`0adfe530 00007ffb`3cc93530 chrome!base::TaskAnnotator::RunTaskImpl+0x1b0
[C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc @ 135]
1b (Inline Function) --------`-------- chrome!base::TaskAnnotator::RunTask+0x191
[C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.h @ 74]
1c (Inline Function) --------`--------
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl+0x39c
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 387]
1d 000000e8`0adfe5f0 00007ffb`3b33fe62
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork+0x440
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 292]
1e 000000e8`0adfe7e0 00007ffb`3a33be6a chrome!base::MessagePumpDefault::Run+0xe2
[C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_default.cc @ 40]
1f 000000e8`0adfe890 00007ffb`3a54ac41
chrome!base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run+0x8a
[C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc @ 502]
20 000000e8`0adfe900 00007ffb`3ada41a1 chrome!base::RunLoop::Run+0x1c1
[C:\b\s\w\ir\cache\builder\src\base\run_loop.cc @ 143]

21 000000e8`0adfea30 00007ffb`3bceed3a chrome!content::GpuMain+0x511
[C:\b\s\w\ir\cache\builder\src\content\gpu\gpu_main.cc @ 403]
22 (Inline Function) --------`-------- chrome!content::RunOtherNamedProcessTypeMain+0x818

22 (Inline Function) -------- -------- chrome!content::RunOtherNamedProcessTypeMain+0x818
[C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc @ 683]
23 000000e8`0adfed40 00007ffb`3a383191 chrome!content::ContentMainRunnerImpl::Run+0xa3a
[C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc @ 1045]
24 (Inline Function) --------`-------- chrome!content::RunContentProcess+0x552
[C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc @ 399]
25 000000e8`0adfef40 00007ffb`3a381087 chrome!content::ContentMain+0x5c1
[C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc @ 427]
26 000000e8`0adff180 00007ff7`3989eba6 chrome!ChromeMain+0x1c7
[C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc @ 179]
27 000000e8`0adff2e0 00007ff7`3989e708 chrome_exe!MainDllLoader::Launch+0x2d6
[C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc @ 167]
28 000000e8`0adff560 00007ff7`39920952 chrome_exe!wWinMain+0xcc8
[C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc @ 382]
29 (Inline Function) --------`-------- chrome_exe!invoke_main+0x21
[d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 118]
2a 000000e8`0adff990 00007ffb`e68b54e0 chrome_exe!__scrt_common_main_seh+0x106
[d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl @ 288]
2b 000000e8`0adff9d0 00007ffb`e7c8485b KERNEL32!BaseThreadInitThunk+0x10
2c 000000e8`0adffa00 00000000`00000000 ntdll!RtlUserThreadStart+0x2b

asan.log
13.2 KB View Download

poc.html
808 bytes View Download

Comment 1 by sheriffbot on Sat, Feb 12, 2022, 4:47 PM EST Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Sun, Feb 13, 2022, 10:54 AM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5764878006288384.

Comment 3 by ClusterFuzz on Sun, Feb 13, 2022, 3:58 PM EST Project Member

Labels: OS-Linux

Comment 4 by ClusterFuzz on Sun, Feb 13, 2022, 6:08 PM EST Project Member

Labels: OS-Android

Comment 5 by ClusterFuzz on Mon, Feb 14, 2022, 6:22 AM EST Project Member

Labels: OS-Mac

Comment 6 by adetaylor@google.com on Mon, Feb 14, 2022, 12:03 PM EST Project Member

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

Cc: spang@google.com jmad...@chromium.org
Labels: FoundIn-98 Security_Severity-High OS-Chrome OS-Fuchsia OS-Windows Pri-1
Components: Internals>GPU

Heap buffer overflow in the GPU process => high severity. ClusterFuzz has identified the regression range as 778057:778060 so tagging as FoundIn-98 (the earliest current release branch). Assuming this affects all non-iOS platforms.

Almost certainly 'regressed' by https://chromium.googlesource.com/chromium/src/+/f8f2c05a9f28e29427020948a605ccf3c229d225, although maybe that just rearranged things to yield a pre-existing bug a different way. Anyway, over to spang@ to work out how to progress this.

jmadill@ please could you take a look too, in case spang@ isn't the right owner?

Comment 7 by sheriffbot on Mon, Feb 14, 2022, 12:18 PM EST Project Member

Labels: Security_Impact-Extended

Comment 8 by sheriffbot on Mon, Feb 14, 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 9 by sheriffbot on Sun, Feb 27, 2022, 12:21 PM EST Project Member

spang: Uh oh! This issue still open and hasn't been updated in the last 14 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 10 by jmad...@chromium.org on Mon, Feb 28, 2022, 2:58 PM EST Project Member

Owner: jmad...@chromium.org

Comment 11 by Git Watcher on Thu, Mar 3, 2022, 3:11 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/348ece42552a99cff88f79c80652b9dd3155ab22

commit 348ece42552a99cff88f79c80652b9dd3155ab22
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the
layer render target in TextureVk::getAttachmentRenderTarget

layer render target in TextureVk::getAttachmentRenderTarget.

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/348ece42552a99cff88f79c80652b9dd3155ab22/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/348ece42552a99cff88f79c80652b9dd3155ab22/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 12 by Git Watcher on Thu, Mar 3, 2022, 8:11 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/9a2188ee5238f9e9d4ddb8d0983179d55d544e54

commit 9a2188ee5238f9e9d4ddb8d0983179d55d544e54
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Fri Mar 04 01:10:18 2022

Roll ANGLE from 7b202392bf9f to b72718d23720 (5 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/7b202392bf9f..b72718d23720

2022-03-03 cclao@google.com Vulkan: Fix the data race for mUse from two threads
2022-03-03 abdolrashidi@google.com Add angle_white_box_tests to SwANGLE tests
2022-03-03 tsniatowski@vewd.com Don't create a string out of a nullptr
2022-03-03 hailinzhang@google.com add host cached bit for staging buffer
2022-03-03 jmadill@chromium.org Vulkan: Fix issue with redefining a layered attachment.

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:1296866~~,chromium:1302724
Tbr: romanl@google.com

Change-Id: Ia15d14b455306d92167a3c29e39a384365013438
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498923
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@{#977440}

[modify] https://crrev.com/9a2188ee5238f9e9d4ddb8d0983179d55d544e54/DEPS

Comment 13 by jmad...@chromium.org on Fri, Mar 4, 2022, 8:14 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 14 by sheriffbot on Fri, Mar 4, 2022, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 15 by sheriffbot on Fri, Mar 4, 2022, 1:41 PM EST Project Member

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

Comment 16 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 (977440) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (977440) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (977440) appears to be after beta branch point (972766).

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

Comment 17 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 18 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 19 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 20 by ClusterFuzz on Mon, Mar 7, 2022, 8:53 AM EST Project Member

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

ClusterFuzz testcase 5764878006288384 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=977439:977443

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

Comment 21 by jmad...@chromium.org on Mon, Mar 7, 2022, 12:32 PM EST Project Member

Cc: -spang@google.com

Comment 22 by jmad...@chromium.org on Mon, Mar 7, 2022, 12:32 PM EST Project Member

1. heap buffer overflow
2. https://chromium-review.googlesource.com/c/angle/angle/+/3498283
3. yes
4. no

Comment 23 by srinivassista@google.com on Mon, Mar 7, 2022, 12:36 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 24 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 25 by eakpobaro@google.com on Tue, Mar 8, 2022, 9:38 AM EST Project Member

[Bulk edit]

This has been approved for merge , please merge ASAP

Comment 26 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/+/faa96536d88a5a9800b416e28c8ef0c4b30a23e4

commit faa96536d88a5a9800b416e28c8ef0c4b30a23e4
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

[M100] Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the
layer render target in TextureVk::getAttachmentRenderTarget.

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 348ece42552a99cff88f79c80652b9dd3155ab22)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3508697
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/faa96536d88a5a9800b416e28c8ef0c4b30a23e4/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/faa96536d88a5a9800b416e28c8ef0c4b30a23e4/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 27 by sheriffbot on Tue, Mar 8, 2022, 9:57 AM EST Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 28 by jmad...@chromium.org on Tue, Mar 8, 2022, 10:01 AM EST Project Member

Cc: geoff...@chromium.org
Labels: -OS-Chrome

I don't think we ship Vulkan ANGLE in M96 on ChromeOS. Geoff can you confirm?

Comment 29 by jmad...@chromium.org on Tue, Mar 8, 2022, 10:01 AM EST Project Member

Labels: -OS-Android

Comment 30 by amyressler@chromium.org on Tue, Mar 8, 2022, 6:23 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 NLT 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 refresh

Comment 31 by rzanoni@google.com on Wed, Mar 9, 2022, 10:28 AM EST Project Member

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 32 by rzanoni@google.com on Wed, Mar 9, 2022, 10:39 AM EST Project Member

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 33 by Git Watcher on Wed, Mar 9, 2022, 10:40 AM EST Project Member

Labels: merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/2b75a29bf241e2e9cefe768415cd30a2109758ae

commit 2b75a29bf241e2e9cefe768415cd30a2109758ae
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

[M96-LTS] Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the
layer render target in TextureVk::getAttachmentRenderTarget.

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e0fad5e766e20580b09336713e675e4e4f0

Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 348ece42552a99cff88f79c80652b9dd3155ab22)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3513754
Reviewed-by: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/2b75a29bf241e2e9cefe768415cd30a2109758ae/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/2b75a29bf241e2e9cefe768415cd30a2109758ae/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 34 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/+/c57eb113c751d17771756a8757410edebf246b12

commit c57eb113c751d17771756a8757410edebf246b12
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

[M99] Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the
layer render target in TextureVk::getAttachmentRenderTarget.

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 348ece42552a99cff88f79c80652b9dd3155ab22)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3514172
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/c57eb113c751d17771756a8757410edebf246b12/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/c57eb113c751d17771756a8757410edebf246b12/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 35 by Git Watcher on Wed, Mar 9, 2022, 11:10 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/+/9e133489f0011e0ff00862ed3429c80006e2dedc

commit 9e133489f0011e0ff00862ed3429c80006e2dedc
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

[M98] Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the

layer render target in TextureVk::getAttachmentRenderTarget.

Bug: chromium:1296866

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 348ece42552a99cff88f79c80652b9dd3155ab22)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3514173
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/9e133489f0011e0ff00862ed3429c80006e2dedc/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/9e133489f0011e0ff00862ed3429c80006e2dedc/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 36 by Git Watcher on Wed, Mar 9, 2022, 11:11 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/c57eb113c751d17771756a8757410edebf246b12

commit c57eb113c751d17771756a8757410edebf246b12
Author: Jamie Madill <jmadill@chromium.org>
Date: Tue Mar 01 20:40:38 2022

[M99] Vulkan: Fix issue with redefining a layered attachment.

The fix ensures we complete level redefinition before we get the
layer render target in TextureVk::getAttachmentRenderTarget.

~~Bug: chromium:1296866~~
Change-Id: Id7fa8e9fed5e766c30580b09336713c675c4e4f0
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3498283
Reviewed-by: Amirali Abdolrashidi <abdolrashidi@google.com>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 348ece42552a99cff88f79c80652b9dd3155ab22)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3514172
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

[modify] https://crrev.com/c57eb113c751d17771756a8757410edebf246b12/src/tests/gl_tests/FramebufferTest.cpp
[modify] https://crrev.com/c57eb113c751d17771756a8757410edebf246b12/src/libANGLE/renderer/vulkan/TextureVk.cpp

Comment 37 by gmpritchard@google.com on Wed, Mar 9, 2022, 1:23 PM EST Project Member

Labels: -LTS-Merge-Candidate -LTS-Merge-Request-96 LTS-Merge-Merged-96

Looks like it was already merged to M96 (without approval) per comment#33. Fixing labels.

Comment 38 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

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 39 by amyressler@chromium.org on Thu, Mar 10, 2022, 10:57 PM EST Project Member

Congratulations! The VRP Panel has decided to award you $7,000 for this report. Thank you for your work discovering GPU bugs and reporting this issue to us!

Comment 40 by amyressler@google.com on Fri, Mar 11, 2022, 2:48 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 41 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:27 PM EST Project Member

Labels: Release-1-M99

Comment 42 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0976 CVE_description-missing

Comment 43 by Git Watcher on Sat, Apr 2, 2022, 1:00 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/535cd538f3585b44855647339f04bae1c1acf63a

commit 535cd538f3585b44855647339f04bae1c1acf63a
Author: Shahbaz Youssefi <syoussefi@chromium.org>
Date: Tue Mar 29 20:29:58 2022

Vulkan: Fix texture-after-framebuffer sync issues

In TextureVk::syncState, for various reasons, the underlying image may need to be respecified. For example because base/max level changed, usage/create flags have changed, the format needs modification to become renderable, generate mipmap is adding levels, etc.

Currently, ANGLE syncs FramebufferVk before TextureVk for the sake of the deferred clear optimization. This means that if the texture needs to recreate its underlying image, it needs to do so earlier than its own syncState, and do so in FramebufferVk::syncState through the TextureVk::getAttachmentRenderTarget function.

Over time, TextureVk::getAttachmentRenderTarget was modified to do parts of what TextureVk::syncState did for this matter as bugs were discovered, and more continue to be discovered. The bug that prompted this change is missing image recreation when usage/create flags change.

In this change, the relevant code in TextureVk::syncState is refactored in a helper that's called by TextureVk::getAttachmentRenderTarget. This way, the two functions should always be in agreement, avoiding TextureVk::syncState recreating the image after FramebufferVk::syncState, leading to use-after-free bugs.

~~Bug: angleproject:4418~~
~~Bug: angleproject:6909~~
Bug: chromium:1266094
~~Bug: chromium:1296866~~
Change-Id: I856a34ca5cf573578c771f5adbeb9208420a3f62
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3557817
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Charlie Lao <cclao@google.com>
Commit-Queue: Shahbaz Youssefi <syoussefi@chromium.org>

[modify]
https://crrev.com/535cd538f3585b44855647339f04bae1c1acf63a/src/tests/deqp_support/deqp_gles31_test_expectations.txt
[modify] https://crrev.com/535cd538f3585b44855647339f04bae1c1acf63a/src/libANGLE/renderer/vulkan/TextureVk.h
[modify] https://crrev.com/535cd538f3585b44855647339f04bae1c1acf63a/src/libANGLE/renderer/vulkan/TextureVk.cpp
[modify]
https://crrev.com/535cd538f3585b44855647339f04bae1c1acf63a/src/tests/deqp_support/deqp_gles3_test_expectations.txt

Comment 44 by Git Watcher on Sat, Apr 2, 2022, 5:47 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b2f7e89dcec58c0376af82d96688ab0c6f4173a1

commit b2f7e89dcec58c0376af82d96688ab0c6f4173a1
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Sat Apr 02 21:46:04 2022

Roll ANGLE from cd9e887aef6b to 535cd538f358 (4 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/cd9e887aef6b..535cd538f358

2022-04-02 syoussefi@chromium.org Vulkan: Fix texture-after-framebuffer sync issues
2022-04-02 syoussefi@chromium.org Skip failing tests on Pixel 6
2022-04-02 jmadill@chromium.org Vulkan: Lift SwS suppressions.
2022-04-02 abdolrashidi@google.com Remove the TODOs regarding multisample buffer age

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 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_opt

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:1266094,~~chromium:1296866~~
Tbr: syoussefi@google.com
Change-Id: I244a041b03547cea7c208292110d03b61e28a6ac
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3565737
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@{#988290}

[modify] https://crrev.com/b2f7e89dcec58c0376af82d96688ab0c6f4173a1/DEPS

Comment 45 by Git Watcher on Mon, Apr 4, 2022, 12:14 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/b33767ec9adef7492b72f78af2f1445db49108ab

commit b33767ec9adef7492b72f78af2f1445db49108ab
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 04 15:26:29 2022

Revert "Vulkan: Fix texture-after-framebuffer sync issues"

This reverts commit 535cd538f3585b44855647339f04bae1c1acf63a.

Reason for revert: May fix Win/Intel blockman_go flakiness.

~~Bug: angleproject:7167~~

Original change's description:
> Vulkan: Fix texture-after-framebuffer sync issues
>
> In TextureVk::syncState, for various reasons, the underlying image may
> need to be respecified. For example because base/max level changed,
> usage/create flags have changed, the format needs modification to become
> renderable, generate mipmap is adding levels, etc.
>
> Currently, ANGLE syncs FramebufferVk before TextureVk for the sake of
> the deferred clear optimization. This means that if the texture needs
> to recreate its underlying image, it needs to do so earlier than its own
> syncState, and do so in FramebufferVk::syncState through the
> TextureVk::getAttachmentRenderTarget function.
>
> Over time, TextureVk::getAttachmentRenderTarget was modified to do parts
> of what TextureVk::syncState did for this matter as bugs were
> discovered, and more continue to be discovered. The bug that prompted
> this change is missing image recreation when usage/create flags change.
>
> In this change, the relevant code in TextureVk::syncState is refactored
> in a helper that's called by TextureVk::getAttachmentRenderTarget. This
> way, the two functions should always be in agreement, avoiding
> TextureVk::syncState recreating the image after
> FramebufferVk::syncState, leading to use-after-free bugs.
>

>
> ~~Bug: angleproject:4418~~
> ~~Bug: angleproject:6909~~
> Bug: chromium:1266094
> ~~Bug: chromium:1296866~~
> Change-Id: I856a34ca5cf573578c771f5adbeb9208420a3f62
> Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3557817
> Reviewed-by: Jamie Madill <jmadill@chromium.org>
> Reviewed-by: Charlie Lao <cclao@google.com>
> Commit-Queue: Shahbaz Youssefi <syoussefi@chromium.org>

~~Bug: angleproject:4418~~
~~Bug: angleproject:6909~~
Bug: chromium:1266094
~~Bug: chromium:1296866~~
Change-Id: I26b6f644442e2875aba954d6417543b1d5121376
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3569801
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Shahbaz Youssefi <syoussefi@chromium.org>
Commit-Queue: Shahbaz Youssefi <syoussefi@chromium.org>

[modify]
https://crrev.com/b33767ec9adef7492b72f78af2f1445db49108ab/src/tests/deqp_support/deqp_gles31_test_expectations.txt
[modify] https://crrev.com/b33767ec9adef7492b72f78af2f1445db49108ab/src/libANGLE/renderer/vulkan/TextureVk.h
[modify] https://crrev.com/b33767ec9adef7492b72f78af2f1445db49108ab/src/libANGLE/renderer/vulkan/TextureVk.cpp
[modify]
https://crrev.com/b33767ec9adef7492b72f78af2f1445db49108ab/src/tests/deqp_support/deqp_gles3_test_expectations.txt

Comment 46 by Git Watcher on Mon, Apr 4, 2022, 4:01 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ce458109a6a93e8a085baff7e6af189b51aa9123

commit ce458109a6a93e8a085baff7e6af189b51aa9123
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Mon Apr 04 19:59:59 2022

Roll ANGLE from bd7915fd0218 to 74eac5e5a506 (3 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/bd7915fd0218..74eac5e5a506

2022-04-04 angle-autoroll@skia-public.iam.gserviceaccount.com Roll VK-GL-CTS from fbc38865227d to 6f8a7182bd26 (14 revisions)
2022-04-04 romanl@google.com Use GTEST_SKIP to set gTest status of skipped tests to SKIPPED.
2022-04-04 jmadill@chromium.org Revert "Vulkan: Fix texture-after-framebuffer sync issues"

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/angle-chromium-autoroll
Please CC jmadill@google.com on the revert to ensure that a human
is aware of the problem.

To file a bug in ANGLE: https://bugs.chromium.org/p/angleproject/issues/entry

To file a bug in 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:1266094,~~chromium:1296866~~
Tbr: jmadill@google.com
Change-Id: I11bf3229d2c350cfd590a3ba6fe6fa0f5f60b549
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3569965
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@{#988631}

[modify] https://crrev.com/ce458109a6a93e8a085baff7e6af189b51aa9123/DEPS

Comment 47 by Git Watcher on Tue, Apr 12, 2022, 2:04 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/aed5951e3b928d537042895226f435f968330b9c

commit aed5951e3b928d537042895226f435f968330b9c
Author: Shahbaz Youssefi <syoussefi@chromium.org>
Date: Tue Mar 29 20:29:58 2022

Reland "Vulkan: Fix texture-after-framebuffer sync issues"

This is a reland of commit 535cd538f3585b44855647339f04bae1c1acf63a

Original change's description:
> Vulkan: Fix texture-after-framebuffer sync issues
>
> In TextureVk::syncState, for various reasons, the underlying image may
> need to be respecified. For example because base/max level changed,
> usage/create flags have changed, the format needs modification to become
> renderable, generate mipmap is adding levels, etc.
>
> Currently, ANGLE syncs FramebufferVk before TextureVk for the sake of
> the deferred clear optimization. This means that if the texture needs
> to recreate its underlying image, it needs to do so earlier than its own
> syncState, and do so in FramebufferVk::syncState through the
> TextureVk::getAttachmentRenderTarget function.
>
> Over time, TextureVk::getAttachmentRenderTarget was modified to do parts
> of what TextureVk::syncState did for this matter as bugs were
> discovered, and more continue to be discovered. The bug that prompted
> this change is missing image recreation when usage/create flags change.
>

>
> In this change, the relevant code in TextureVk::syncState is refactored
> in a helper that's called by TextureVk::getAttachmentRenderTarget. This
> way, the two functions should always be in agreement, avoiding
> TextureVk::syncState recreating the image after
> FramebufferVk::syncState, leading to use-after-free bugs.
>
> ~~Bug: angleproject:4418~~
> ~~Bug: angleproject:6909~~
> Bug: chromium:1266094
> ~~Bug: chromium:1296866~~
> Change-Id: I856a34ca5cf573578c771f5adbeb9208420a3f62
> Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3557817
> Reviewed-by: Jamie Madill <jmadill@chromium.org>
> Reviewed-by: Charlie Lao <cclao@google.com>
> Commit-Queue: Shahbaz Youssefi <syoussefi@chromium.org>

~~Bug: angleproject:4418~~
~~Bug: angleproject:6909~~
Bug: chromium:1266094
~~Bug: chromium:1296866~~
Change-Id: I0110eab88eb9d8f77e204b84a6e90308e2384fd7
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3572715
Reviewed-by: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Yuxin Hu <yuxinhu@google.com>
Commit-Queue: Shahbaz Youssefi <syoussefi@chromium.org>

[modify] https://crrev.com/aed5951e3b928d537042895226f435f968330b9c/src/libANGLE/renderer/vulkan/ImageVk.cpp
[modify] https://crrev.com/aed5951e3b928d537042895226f435f968330b9c/src/tests/deqp_support/deqp_gles31_test_expectations.txt
[modify] https://crrev.com/aed5951e3b928d537042895226f435f968330b9c/src/libANGLE/renderer/vulkan/TextureVk.h
[modify] https://crrev.com/aed5951e3b928d537042895226f435f968330b9c/src/libANGLE/renderer/vulkan/TextureVk.cpp
[modify] https://crrev.com/aed5951e3b928d537042895226f435f968330b9c/src/tests/deqp_support/deqp_gles3_test_expectations.txt

Comment 48 by Git Watcher on Tue, Apr 12, 2022, 6:13 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/15aaa5a53faa8d7d0378452d152915a8e7984b7e

commit 15aaa5a53faa8d7d0378452d152915a8e7984b7e
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Tue Apr 12 10:12:16 2022

Roll ANGLE from 797e627e641c to aed5951e3b92 (1 revision)

https://chromium.googlesource.com/angle/angle.git/+log/797e627e641c..aed5951e3b92

2022-04-12 syoussefi@chromium.org Reland "Vulkan: Fix texture-after-framebuffer sync issues"

If this roll has caused a breakage, revert this CL and stop the roller
using the controls here:
https://autoroll.skia.org/r/angle-chromium-autoroll

https://autoroll.skia.org/r/angle-chromium-autoroll
Please CC jonahr@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:1266094,~~chromium:1296866~~
Tbr: jonahr@google.com
Change-Id: I94a49386dda5f9f26b34b09541e268f0d3c5f97d
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3583571
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@{#991443}

[modify] https://crrev.com/15aaa5a53faa8d7d0378452d152915a8e7984b7e/DEPS

Comment 49 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 50 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 51 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:15 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing