Starred by 5 users

Owner:	jmad...@chromium.org
CC:	ynovikov@chromium.org kbr@chromium.org rzanoni@google.com geoff...@chromium.org syoussefi@chromium.org jmad...@chromium.org
Status:	Verified *(Closed)*
Components:	Internals>GPU>ANGLE
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Needs-Feedback
Security_Severity-High
allpublic
reward-inprocess
ClusterFuzz-Verified
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-99
reward-7000
Target-99
FoundIn-99
Security_Impact-Extended
LTS-NotApplicable-96
merge-merged-4896
merge-merged-100
merge-merged-4951
merge-merged-101
Release-0-M101
CVE-2022-1479

Issue 1305190: [ANGLE] Vulkan Use After Free in onBeginTransformFeedback
Reported by sjh...@gmail.com on Thu, Mar 10, 2022, 8:52 AM EST

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4934.0 Safari/537.36

Steps to reproduce the problem:
1. run with ./chrome --no-sandbox http://localhost:8000/poc1.html
2.
3.

What is the expected behavior?

What went wrong?
Title
- [ANGLE] Vulkan Use After Free in onBeginTransformFeedback

Test Environment
- OS : Ubuntu 20.04 64 bit
- Chromium Version : 101.0.4934.0 (Developer Build) (64-bit)
- Revision : 281980ccda2381e557cf502d101d1be3a0d76352-refs/heads/main@{#979210}
- run option :
  ./chrome --no-sandbox http://localhost:8000/poc1.html

Analysis

* third_party/angle/src/libANGLE/renderer/vulkan/ContextVk.cpp:4815
```c++
angle::Result ContextVk::onBeginTransformFeedback(
    size_t bufferCount,
    const gl::TransformFeedbackBuffersArray<vk::BufferHelper *> &buffers,
    const gl::TransformFeedbackBuffersArray<vk::BufferHelper> &counterBuffers)
{
    onTransformFeedbackStateChanged();

    bool shouldEndRenderPass = false;

    // If any of the buffers were previously used in the render pass, break the render pass as a
    // barrier is needed.
    for (size_t bufferIndex = 0; bufferIndex < bufferCount; ++bufferIndex)
    {
        const vk::BufferHelper *buffer = buffers[bufferIndex];
        if (mRenderPassCommands->usesBuffer(*buffer)) //[*] Here, refers to the already freed buffer.
        {
            shouldEndRenderPass = true;
            break;
        }

    }
//...
```

In above [*], reference to already freed Buffer Object.

Credits
- Jeonghoon Shin at Theori

PoC
- attached poc1.html
ASAN Log
- attached poc1_asan.txt

Did this work before? N/A

Chrome version: 101.0.4934.0 Channel: dev
OS Version: Ubuntu 20.04

report1.md
1.3 KB View Download

poc1.html
2.2 KB View Download

poc1_asan.txt
17.2 KB View Download

Comment 1 by sheriffbot on Thu, Mar 10, 2022, 8:55 AM EST Project Member

Labels: external_security_report

Comment 2 by bookholt@chromium.org on Thu, Mar 10, 2022, 8:30 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: geoff...@chromium.org
Cc: jmad...@chromium.org kbr@chromium.org syoussefi@chromium.org ynovikov@chromium.org
Labels: Security_Severity-High FoundIn-99 OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows OS-Lacros
Components: Internals>GPU>Vulkan Internals>GPU>ANGLE

Thanks for the report!

Successful repro on Linux ASAN build from tip of tree. I only tested a Linux build, but based on the build rules for this file this code is present everywhere except iOS.

Assigning Severity High because UAF in sandbox process can be assumed to lead to RCE.

Comment 3 by sheriffbot on Thu, Mar 10, 2022, 8:35 PM EST Project Member

Labels: Security_Impact-Stable

Comment 4 by ClusterFuzz on Thu, Mar 10, 2022, 11:26 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5760301630554112.

Comment 5 by sheriffbot on Fri, Mar 11, 2022, 12:47 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 6 by sheriffbot on Fri, Mar 11, 2022, 1:08 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 7 by jmad...@chromium.org on Mon, Mar 14, 2022, 9:44 AM EDT Project Member

Owner: jmad...@chromium.org
Labels: -OS-Android

Comment 8 by jmad...@chromium.org on Mon, Mar 14, 2022, 10:36 AM EDT Project Member

~~Issue 1305219~~ has been merged into this issue.

Comment 9 by jmad...@chromium.org on Mon, Mar 14, 2022, 10:36 AM EDT Project Member

Status: Started (was: Assigned)

Comment 10 by jmad...@chromium.org on Mon, Mar 14, 2022, 10:39 AM EDT Project Member

Components: -Internals>GPU>Vulkan

Comment 11 by Git Watcher on Mon, Mar 14, 2022, 5:24 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/708ce9cfd63bc8eab7c48987612a2dedce78c69a

commit 708ce9cfd63bc8eab7c48987612a2dedce78c69a
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Mar 14 14:37:31 2022

Fix crash when pausing XFB then deleting a buffer.

Fix is to validate XFB buffer bindings even if we're paused.
This is undefined behaviour so we can use any non-crashing solution.

~~Bug: chromium:1305190~~
Change-Id: Ib95404cdb13adbde7f34d6cc77473a8b3cbf1de7
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3522283
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/708ce9cfd63bc8eab7c48987612a2dedce78c69a/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/708ce9cfd63bc8eab7c48987612a2dedce78c69a/src/libANGLE/validationES.cpp

Comment 12 by Git Watcher on Wed, Mar 16, 2022, 8:46 PM EDT Project Member

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

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

Roll ANGLE from 3739a195c2df to d867ddbbb1b8 (26 revisions)

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

2022-03-16 m.maiya@samsung.com Doc: Update supported EGL minor version
2022-03-16 yuxinhu@google.com Revert "Flush the texture staged updates when destroying context share group"
2022-03-16 lubosz.sarnecki@collabora.com FrameCapture: Add override for Glsizei* types.
2022-03-16 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-16 romanl@google.com angle_system_info_test also exports androidSdkLevel
2022-03-16 romanl@google.com angle_system_info_test passes json via file
2022-03-16 angle-autoroll@skia-public.iam.gserviceaccount.com Roll vulkan-deps from a11411926c31 to 51988dcdccbf (9 revisions)
2022-03-16 yahan@google.com Do not copy parent layer frame position
2022-03-15 cclao@google.com Vulkan: Update mCurrentElementArrayBuffersync based on dirty bit
2022-03-15 yuxinhu@google.com Flush the texture staged updates when destroying context share group
2022-03-15 b.schade@samsung.com Remove invalid validation check on compressed texture formats
2022-03-15 cclao@google.com Vulkan: Handle the case where the bound buffer is empty
2022-03-15 lubosz.sarnecki@collabora.com FrameCapture: Skip invalid VertexAttribPointer calls in MEC.
2022-03-15 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-15 jmadill@chromium.org Vulkan: Temporarily suppress 3 perf counter tests on P6.
2022-03-15 jmadill@chromium.org Revert "Vulkan: VkFormat/DrmFourCC"
2022-03-15 lexa.knyazev@gmail.com Skip no-op base instance draw calls
2022-03-15 lexa.knyazev@gmail.com Fix typo in DrawElementsInstancedBaseVertexBaseInstanceANGLE
2022-03-15 angle-autoroll@skia-public.iam.gserviceaccount.com Roll Chromium from ffa866a5ae9e to 45902868a797 (562 revisions)
2022-03-15 b.schade@samsung.com Add usage of Spirv through glslang build flag
2022-03-14 kkinnunen@apple.com Add device id as a part of the key in EGLDisplay cache
2022-03-14 antonio.caggiano@collabora.com Vulkan: VkFormat/DrmFourCC
2022-03-14 angle-autoroll@skia-public.iam.gserviceaccount.com Roll vulkan-deps from 2d9abfbddc1b to a11411926c31 (18 revisions)
2022-03-14 jmadill@chromium.org Fix crash when pausing XFB then deleting a buffer.
2022-03-14 cclao@google.com Vulkan: Fix another corner case of mCurrentElementArrayBuffer
2022-03-14 angle-autoroll@skia-public.iam.gserviceaccount.com Roll VK-GL-CTS from f7e842466e0a to 8252a3d3cdd3 (8 revisions)

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

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

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

To report a problem with the AutoRoller itself, please file a bug:

To report a problem with the AutoRoller itself, please file a bug:
https://bugs.chromium.org/p/skia/issues/entry?template=Autoroller+Bug

Documentation for the AutoRoller is here:
https://skia.googlesource.com/buildbot/+doc/main/autoroll/README.md

Cq-Include-Trybots:
luci.chromium.try:android_optional_gpu_tests_rel;luci.chromium.try:linux_optional_gpu_tests_rel;luci.chromium.try:mac_optional_gpu_tests_rel;luci.chromium.try:win_optional_gpu_tests_rel;luci.chromium.try:linux-swangle-try-x64;luci.chromium.try:win-swangle-try-x86
~~Bug: chromium:1296467~~,~~chromium:1299211~~,~~chromium:1299261~~,~~chromium:1305190~~
Tbr: jmadill@google.com
Test: Test: angle_end2end_tests --gtest_filter="VertexAttributeTestES3.InvalidAttribPointer/*"
Test: Test: capture_replay_tests.py --gtest_filter=FenceSyncTest.NullLength/*
Test: Test: gtest_filter=*DXT1CompressedTextureTest.NonBlockSizesMipLevels*
Test: Test: when using ANGLE (with metal or swiftshader backend) with
Change-Id: I52ffe787d20dd083af8efe1bdef05616ac611f55
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3530116
Commit-Queue: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Bot-Commit: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Cr-Commit-Position: refs/heads/main@{#981945}

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

Comment 13 by adetaylor@google.com on Mon, Mar 21, 2022, 2:48 PM EDT Project Member

Cc: geoff...@chromium.org

(auto-cc on security bug)

Comment 14 by sjh...@gmail.com on Mon, Mar 28, 2022, 10:58 PM EDT

Hi.

Is this issue already fixed?

Thanks

Comment 15 by sheriffbot on Tue, Mar 29, 2022, 2:19 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 16 by jmad...@chromium.org on Wed, Mar 30, 2022, 9:10 AM EDT Project Member

Status: Fixed (was: Started)

Yes, it's fixed, thanks for the ping.

Comment 17 by sheriffbot on Wed, Mar 30, 2022, 12:45 PM EDT Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Wed, Mar 30, 2022, 1:44 PM EDT Project Member

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

Comment 19 by jmad...@chromium.org on Mon, Apr 11, 2022, 11:40 AM EDT Project Member

Should this fix be merged?

Comment 20 by jmad...@chromium.org on Mon, Apr 11, 2022, 11:41 AM EDT Project Member

~~Issue 1313905~~ has been merged into this issue.

Comment 21 by ClusterFuzz on Mon, Apr 11, 2022, 11:45 AM EDT Project Member

Labels: Needs-Feedback

ClusterFuzz testcase 6205249010073600 is still reproducing on tip-of-tree build (trunk).

Please re-test your fix against this testcase and if the fix was incorrect or incomplete, please re-open the bug. Otherwise, ignore this notification and add the ClusterFuzz-Wrong label.

Comment 22 by amyressler@google.com on Mon, Apr 11, 2022, 1:06 PM EDT Project Member

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

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. 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 23 by amyressler@chromium.org on Mon, Apr 11, 2022, 1:27 PM EDT Project Member

Congratulations, Jeonghoon! The VRP Panel has decided to award you $7,000 for this report. Thank you for your efforts and nice work!

Comment 24 by Git Watcher on Mon, Apr 11, 2022, 5:22 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/5c85fd4e11a3835a0719223a7cedb978d309da21

commit 5c85fd4e11a3835a0719223a7cedb978d309da21
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Apr 11 16:29:00 2022

Add error check on resuming XFB with deleted buffer.

~~Bug: chromium:1305190~~
Change-Id: I22c6f6400b05ca32c922fba9a3b9d4b5841ca8b8
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3578378
Auto-Submit: Jamie Madill <jmadill@chromium.org>
Reviewed-by: Geoff Lang <geofflang@chromium.org>

Commit-Queue: Jamie Madill <jmadill@chromium.org>

[modify] https://crrev.com/5c85fd4e11a3835a0719223a7cedb978d309da21/src/tests/gl_tests/TransformFeedbackTest.cpp

[modify] https://crrev.com/5c85fd4e11a3835a0719223a7cedb978d309da21/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/5c85fd4e11a3835a0719223a7cedb978d309da21/src/libANGLE/validationES3.cpp

Comment 25 by sjh...@gmail.com on Mon, Apr 11, 2022, 6:13 PM EDT

thanks for the reward!

Comment 26 by Git Watcher on Tue, Apr 12, 2022, 12:43 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/12e39e60c7b15f677b8f6776d9922b52d4a98ca6

commit 12e39e60c7b15f677b8f6776d9922b52d4a98ca6
Author: chromium-autoroll <chromium-autoroll@skia-public.iam.gserviceaccount.com>
Date: Tue Apr 12 04:42:05 2022

Roll ANGLE from a947c5f56cf7 to eeb396535317 (6 revisions)

https://chromium.googlesource.com/angle/angle.git/+log/a947c5f56cf7..eeb396535317

2022-04-12 syoussefi@chromium.org Autogenerate features
2022-04-12 gman@chromium.org Metal:remove TextureMtl::mIsPow2
2022-04-11 kkinnunen@apple.com Metal: Avoid leaking MTLDevice lists in DisplayMtl
2022-04-11 kkinnunen@apple.com Metal: Avoid leaking MTLFunctionConstantValues in ProgramMtl
2022-04-11 steven@valvesoftware.com egl_angle_ext.xml: add missing enums and typedefs
2022-04-11 jmadill@chromium.org Add error check on resuming XFB with deleted buffer.

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 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:1305190~~
Tbr: jonahr@google.com
Change-Id: Iccec53b895433a13ca65f021622de2ad666531d1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3583202
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@{#991364}

[modify] https://crrev.com/12e39e60c7b15f677b8f6776d9922b52d4a98ca6/DEPS

[modify] https://crrev.com/12e396b0c7b15b77b8b77bd9922b52d4a98cab/DEPS

Comment 27 by ClusterFuzz on Tue, Apr 12, 2022, 5:29 PM EDT Project Member

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

ClusterFuzz testcase 6205249010073600 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=991358:991364

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

Comment 28 by amyressler@google.com on Tue, Apr 12, 2022, 9:10 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 29 by amyressler@chromium.org on Fri, Apr 15, 2022, 3:39 PM EDT Project Member

Labels: Merge-Request-101 Merge-Request-100

Manually adding merge request labels so these go into merge review queue (we are also looking into why sheriffbot is sleeping on the job in this regard)

Comment 30 by sheriffbot on Fri, Apr 15, 2022, 3:41 PM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

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), matthewjoseph (ChromeOS), pbommana (Desktop)

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

Comment 31 by sheriffbot on Fri, Apr 15, 2022, 3:41 PM EDT Project Member

Labels: -Merge-Request-100 Merge-Review-100

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

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches

- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?

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

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

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

Comment 32 by amyressler@chromium.org on Fri, Apr 15, 2022, 8:35 PM EDT Project Member

Labels: -Merge-Review-100 -Merge-Review-101 Merge-Approved-100 Merge-Approved-101

m101 merge approved, please merge this fix to branch 4951
m100 merge approved, please merge this fix to branch 4896
please complete both merges prior to 10am PDT, Tuesday 19 April so this fix can be included in the m101 and m100 stable and extended stable cuts

Comment 33 by amyressler@chromium.org on Fri, Apr 15, 2022, 8:40 PM EDT Project Member

I should have specified, both CLs (https://chromium-review.googlesource.com/c/angle/angle/+/3578378 and https://chromium-review.googlesource.com/c/angle/angle/+/3522283) to M100

https://chromium-review.googlesource.com/c/angle/angle/+/3522283 is already on M101, so please merge https://chromium-review.googlesource.com/c/angle/angle/+/3578378 to M101

thanks!

Comment 34 by Git Watcher on Tue, Apr 19, 2022, 10:17 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/angle/angle/+/d24570fb658ef04f67c773989af6218ff8a3a7a6

commit d24570fb658ef04f67c773989af6218ff8a3a7a6
Author: Jamie Madill <jmadill@chromium.org>
Date: Mon Mar 14 14:37:31 2022

[M100] Fix crash when pausing XFB then deleting a buffer.

Fix is to validate XFB buffer bindings even if we're paused.
This is undefined behaviour so we can use any non-crashing solution.

~~Bug: chromium:1305190~~
Change-Id: Ib95404cdb13adbde7f34d6cc77473a8b3cbf1de7
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3522283
Reviewed-by: Geoff Lang <geofflang@chromium.org>
Commit-Queue: Jamie Madill <jmadill@chromium.org>
(cherry picked from commit 708ce9cfd63bc8eab7c48987612a2dedce78c69a)
Reviewed-on: https://chromium-review.googlesource.com/c/angle/angle/+/3594105
Reviewed-by: Shahbaz Youssefi <syoussefi@chromium.org>

[modify] https://crrev.com/d24570fb658ef04f67c773989af6218ff8a3a7a6/src/tests/gl_tests/TransformFeedbackTest.cpp

[modify] https://crrev.com/d24570fb658ef04f67c773989af6218ff8a3a7a6/src/tests/gl_tests/TransformFeedbackTest.cpp
[modify] https://crrev.com/d24570fb658ef04f67c773989af6218ff8a3a7a6/src/libANGLE/validationES.cpp

Comment 35 by sheriffbot on Tue, Apr 19, 2022, 10:17 AM EDT Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

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

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

Comment 36 by pbommana@google.com on Tue, Apr 19, 2022, 10:26 AM EDT Project Member

Labels: -Merge-Approved-101 Merge-merged-101 Merge-merged-4951

Based on offline chat we have all the Merged to M101 hence marking the merge labels manually

Comment 37 by rzanoni@google.com on Tue, Apr 19, 2022, 1:22 PM EDT Project Member

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

Changed code is not present in M96.

Comment 38 by amyressler@chromium.org on Mon, Apr 25, 2022, 7:04 PM EDT Project Member

Labels: Release-0-M101

Comment 39 by amyressler@google.com on Tue, Apr 26, 2022, 4:30 PM EDT Project Member

Labels: CVE-2022-1479 CVE_description-missing

Comment 40 by sheriffbot on Wed, Jul 6, 2022, 1:30 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 41 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 42 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing