Starred by 3 users

Owner:	shrekshao@google.com
CC:	kbr@chromium.org adetaylor@chromium.org prashanthpola@chromium.org shrekshao@google.com jbroman@chromium.org jdarpinian@chromium.org achuith@chromium.org
Status:	Verified *(Closed)*
Components:	Blink>Workers Blink>WebGL
Modified:	May 28, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Stability-Crash
Security_Impact-Stable
Security_Severity-High
ReleaseBlock-Stable
allpublic
reward-inprocess
ClusterFuzz-Verified
CVE_description-submitted
M-81
Target-81
VulnerabilityAnalysis-Requested
merge-merged-3987
merge-merged-80
merge-merged-4044
merge-merged-81
reward-8500
CVE-2020-6422
merge-merged-3987_137
Release-5-M80

Issue 1051748: Use-after-poison in WebGLRenderingContextBase

Reported by da...@davidmanouchehri.com on Wed, Feb 12, 2020, 7:39 PM EST

Code

VULNERABILITY DETAILS
Inside WebGLRenderingContextBase::PrintWarningToConsole, we can end up in a state where a garbage collected context is used.

We can trigger this edge case through the following steps:

1. Create an iframe and append it to our document to get a new ExecutionContext
2. Create a AudioWorklet within our new iframe's ExecutionContext
3. Remove the iframe's ExecutionContext, which calls ContextLifecycleObserver::ContextDestroyed
4. Force a WebGL console error message, which will attempt to use the context that was uninitialized

```
void WebGLRenderingContextBase::PrintWarningToConsole(const String& message) {
  blink::ExecutionContext* context = Host()->GetTopExecutionContext();
  if (context) { // <---------------- UAP, does not check if the context has been destroyed
    context->AddConsoleMessage(
        ConsoleMessage::Create(mojom::ConsoleMessageSource::kRendering,
                               mojom::ConsoleMessageLevel::kWarning, message));
  }
}
```

Note: I'm simply using AudioWorklets because I'm already familiar with them, I don't think there's a bug here in WebAudio. I would expect other Worklet interfaces to be able to trigger the same bug.

VERSION
Tested on 79.0.3945.130 + stable and 82.0.4057.0 + canary
Operating System: Any

REPRODUCTION CASE
Put audio.html, audio.js, and processor.js in the same folder, then serve that folder over HTTPS. Open https://localhost:44444/audio.html (replace with applicable port/host) in Chrome.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: Tab/renderer
Crash State:
[0212/191530.862516:ERROR:buffer_manager.cc(817)] [.WebGL-0x61b000063580]GL ERROR :GL_INVALID_VALUE : glMapBufferRange: bound to target 0x8892 : offset/size out of range
Received signal 11 SEGV_MAPERR 000000000048
#0 0x5576b998632b in backtrace /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/../sanitizer_common/sanitizer_common_interceptors.inc:4107:13
#1 0x5576c4159e89 in base::debug::CollectStackTrace(void**, unsigned long) ./../../base/debug/stack_trace_posix.cc:840:39
#2 0x5576c3f1b0c3 in base::debug::StackTrace::StackTrace(unsigned long) ./../../base/debug/stack_trace.cc:206:12
#3 0x5576c3f1b0c3 in base::debug::StackTrace::StackTrace() ./../../base/debug/stack_trace.cc:203:28
#4 0x5576c4158aba in base::debug::(anonymous namespace)::StackDumpSignalHandler(int, siginfo_t*, void*) ./../../base/debug/stack_trace_posix.cc:345:3

```
    #5 0x7f2d9b55a890 in __funlockfile ??:?
    #6 0x7f2d9b55a890 in ?? ??:0
    #7 0x5576d235f4a6 in blink::WorkerThread::GetWorkerReportingProxy() const ./../../third_party/blink/renderer/core/workers/worker_thread.h:0:12
    #8 0x5576d235f4a6 in blink::WorkletGlobalScope::AddConsoleMessageImpl(blink::ConsoleMessage*, bool)
./../../third_party/blink/renderer/core/workers/worklet_global_scope.cc:149:19
    #9 0x5576d397d93d in blink::ExecutionContext::AddConsoleMessage(blink::ConsoleMessage*, bool)
./../../third_party/blink/renderer/core/execution_context/execution_context.h:231:5
    #10 0x5576d397d93d in blink::WebGLRenderingContextBase::PrintWarningToConsole(WTF::String const&)
./../../third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc:7609:14
    #11 0x5576d397d93d in blink::WebGLRenderingContextBase::PrintGLErrorToConsole(WTF::String const&)
./../../third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc:7596:3
    #12 0x5576d397a2ca in blink::WebGLRenderingContextBase::OnErrorMessage(char const*, int)
./../../third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc:1434:5
    #13 0x5576c7622fda in base::RepeatingCallback<void (char const*, int)>::Run(char const*, int) const & ./../../base/callback.h:132:12
    #14 0x5576c7622fda in gpu::gles2::GLES2Implementation::SendErrorMessage(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >, int)
./../../gpu/command_buffer/client/gles2_implementation.cc:414:27
    #15 0x5576c7622c09 in gpu::gles2::GLES2Implementation::OnGpuControlErrorMessage(char const*, int) ./../../gpu/command_buffer/client/gles2_implementation.cc:373:3
    #16 0x5576bb5de455 in void base::DispatchToMethodImpl<gpu::CommandBufferProxyImpl*, void (gpu::CommandBufferProxyImpl::*)
(GPUCommandBufferConsoleMessage const&), std::__1::tuple<GPUCommandBufferConsoleMessage>, 0ul>(gpu::CommandBufferProxyImpl* const&, void
(gpu::CommandBufferProxyImpl::*)(GPUCommandBufferConsoleMessage const&), std::__1::tuple<GPUCommandBufferConsoleMessage>&&,
std::__1::integer_sequence<unsigned long, 0ul>) ./../../base/tuple.h:52:3
    #17 0x5576bb5de455 in void base::DispatchToMethod<gpu::CommandBufferProxyImpl*, void (gpu::CommandBufferProxyImpl::*)(GPUCommandBufferConsoleMessage
const&), std::__1::tuple<GPUCommandBufferConsoleMessage> >(gpu::CommandBufferProxyImpl* const&, void (gpu::CommandBufferProxyImpl::*)
(GPUCommandBufferConsoleMessage const&), std::__1::tuple<GPUCommandBufferConsoleMessage>&&) ./../../base/tuple.h:60:3
    #18 0x5576bb5de455 in void IPC::DispatchToMethod<gpu::CommandBufferProxyImpl, void (gpu::CommandBufferProxyImpl::*)(GPUCommandBufferConsoleMessage
const&), void, std::__1::tuple<GPUCommandBufferConsoleMessage> >(gpu::CommandBufferProxyImpl*, void (gpu::CommandBufferProxyImpl::*)
(GPUCommandBufferConsoleMessage const&), void*, std::__1::tuple<GPUCommandBufferConsoleMessage>&&) ./../../ipc/ipc_message_templates.h:51:3
    #19 0x5576bb5de455 in bool IPC::MessageT<GpuCommandBufferMsg_ConsoleMsg_Meta, std::__1::tuple<GPUCommandBufferConsoleMessage>,
void>::Dispatch<gpu::CommandBufferProxyImpl, gpu::CommandBufferProxyImpl, void, void (gpu::CommandBufferProxyImpl::*)(GPUCommandBufferConsoleMessage
const&)>(IPC::Message const*, gpu::CommandBufferProxyImpl*, gpu::CommandBufferProxyImpl*, void*, void (gpu::CommandBufferProxyImpl::*)
(GPUCommandBufferConsoleMessage const&)) ./../../ipc/ipc_message_templates.h:146:7
    #20 0x5576bb5dd645 in gpu::CommandBufferProxyImpl::OnMessageReceived(IPC::Message const&) ./../../gpu/ipc/client/command_buffer_proxy_impl.cc:144:5
    #21 0x5576c4029773 in base::OnceCallback<void ()>::Run() && ./../../base/callback.h:98:12
    #22 0x5576c4029773 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) ./../../base/task/common/task_annotator.cc:142:33
    #23 0x5576c4062619 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*, bool*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:365:23
    #24 0x5576c4061f9a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoSomeWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:219:7
    #25 0x5576c3f6ac4e in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39:55
    #26 0x5576c4064403 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:463:12
    #27 0x5576c4064403 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #28 0x5576c3fd8c7b in base::RunLoop::Run() ./../../base/run_loop.cc:124:14
    #29 0x5576c21e4f32 in blink::scheduler::WorkerThread::SimpleThreadImpl::Run() ./../../third_party/blink/renderer/platform/scheduler/worker/worker_thread.cc:169:14
    #30 0x5576c4191632 in base::(anonymous namespace)::ThreadFunc(void*) ./../../base/threading/platform_thread_posix.cc:81:13
    #31 0x7f2d9b54f6db in start_thread ??:0:0
    #32 0x7f2d93d6188f in clone ??:0:0
  r8: 7fffffffffffffff  r9: 00007f2d77e39864 r10: 00007f2d79146f50 r11: 00000fd7ad71c3e2
 r12: 00007ecb2a861a98 r13: 00000fd96550c3db r14: 00007ecb2a861ed8 r15: 00007eb96b921ec8
  di: 0000000000000048  si: 00007eb96b921ec8  bp: 00007f2d79147090  bx: 00007f2d791470a0
  dx: 0000000000000000  ax: 0000000000000009  cx: 00005576d639e660  sp: 00007f2d79147050
  ip: 00005576d235f4a6 efl: 0000000000010246 cgf: 002b000000000033 erf: 0000000000000004
 trp: 000000000000000e msk: 0000000000000000 cr2: 0000000000000048
[end of stack trace]
```

CREDIT INFORMATION
Reporter credit: David Manouchehri

[Deleted]	**audio.js**
[Deleted]	**processor.js**
[Deleted]	**audio.html**

Comment 1 by da...@davidmanouchehri.com on Wed, Feb 12, 2020, 7:41 PM EST

The primitive gained is the same as https://bugs.chromium.org/p/chromium/issues/detail?id=1048473.

I'm going to take a stab at patching this one myself. =)

Comment 2 Deleted

Comment 3 by da...@davidmanouchehri.com on Wed, Feb 12, 2020, 8:01 PM EST

I've patched the vulnerability for ya, no longer crashes on the UAP. https://chromium-review.googlesource.com/c/chromium/src/+/2053167

Comment 4 by da...@davidmanouchehri.com on Wed, Feb 12, 2020, 9:03 PM EST

Could @shrekshao be added to this ticket? I believe he's looked at similar bugs before.

Comment 5 by rsleevi@chromium.org on Thu, Feb 13, 2020, 11:00 AM EST

Cc: shrekshao@google.com
Components: Blink>WebGL

Comment 6 by ClusterFuzz on Thu, Feb 13, 2020, 12:56 PM EST

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5644307466878976.

Comment 7 by ClusterFuzz on Thu, Feb 13, 2020, 3:15 PM EST

Labels: Unreproducible

ClusterFuzz testcase 5644307466878976 appears to be flaky, updating reproducibility label.

Comment 8 by ClusterFuzz on Thu, Feb 13, 2020, 3:15 PM EST

Detailed Report: https://clusterfuzz.com/testcase?key=5644307466878976

Fuzzer:
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Null-dereference READ
Crash Address: 0x000000000048

Crash State:
  blink::WorkletGlobalScope::AddConsoleMessageImpl
  blink::WebGLRenderingContextBase::PrintWarningToConsole
  blink::WebGLRenderingContextBase::PrintGLErrorToConsole

Sanitizer: address (ASAN)

Crash Revision: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&revision=741099

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5644307466878976

Additional requirements: Requires HTTP

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5644307466878976 -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

********** UNREPRODUCIBLE **********
Note: This crash might not be reproducible with the provided testcase. That said, for the past 14 days, we've been seeing this crash frequently.

It may be possible to reproduce by trying the following options:
- Run testcase multiple times for a longer duration.
- Run fuzzing without testcase argument to hit the same crash signature.

If it still does not reproduce, try a speculative fix based on the crash stacktrace and verify if it works by looking at the crash statistics in the report. We will auto-close the bug if the crash is not seen for 14 days.
****

Comment 9 by da...@davidmanouchehri.com on Thu, Feb 13, 2020, 3:27 PM EST

I rebased my CL and confirmed that the UAP does not occur locally anymore. Not sure what ClusterFuzz is up to.

Comment 10 by rsleevi@chromium.org on Mon, Feb 17, 2020, 11:16 AM EST

Cc: jdarpinian@chromium.org jbroman@chromium.org

Comment 11 by rsleevi@chromium.org on Mon, Feb 17, 2020, 11:26 AM EST

Status: Assigned (was: Unconfirmed)
Owner: shrekshao@google.com
Labels: Stability-Crash Security_Impact-Stable Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
Components: Blink>Workers

shrekshao: Could you look at this? This seems related to ~~Issue 1098399~~, and it looks like it may be a worker race condition triggering whether or not it will be a NULL deref or something else. I'm tentatively targeting it Medium, but it may be a high if it ends up as a UAP?

I can reproduce it as a crash on HEAD, kicked off clusterfuzz again.

Comment 12 by sheriffbot on Mon, Feb 17, 2020, 11:28 AM EST

Labels: Target-81 M-81

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

Comment 13 by sheriffbot on Mon, Feb 17, 2020, 12:04 PM EST

Labels: Pri-1

Setting Pri-1 to match security severity Medium. 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 14 by ClusterFuzz on Mon, Feb 17, 2020, 10:14 PM EST

Labels: -Security_Impact-Stable Security_Impact-Head

Detailed Report: https://clusterfuzz.com/testcase?key=5644307466878976

Fuzzer:
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Null-dereference READ
Crash Address: 0x000000000048
Crash State:
  blink::WorkletGlobalScope::AddConsoleMessageImpl
  blink::WebGLRenderingContextBase::PrintWarningToConsole
  blink::WebGLRenderingContextBase::PrintGLErrorToConsole

Sanitizer: address (ASAN)

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=668438:668440

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5644307466878976

Additional requirements: Requires HTTP

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone https://github.com/google/clusterfuzz && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t https://clusterfuzz.com/testcase-detail/5644307466878976 -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 15 by da...@davidmanouchehri.com on Tue, Feb 18, 2020, 9:59 AM EST

Could you try applying my patch? It's pretty simple and should solve the problem. https://chromium-review.googlesource.com/c/chromium/src/+/2053167

Comment 16 by sheriffbot on Tue, Feb 18, 2020, 10:52 AM EST
Labels: -Security_Impact-Head Security_Impact-Beta

Comment 17 by shrekshao@google.com on Tue, Feb 18, 2020, 1:56 PM EST
Cc: kbr@chromium.org

Comment 18 by shrekshao@google.com on Tue, Feb 18, 2020, 5:27 PM EST
Labels: -Unreproducible

Comment 19 by bugdroid on Tue, Feb 18, 2020, 7:31 PM EST
The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/54454ec7fbcbd043f7eafea03049e53ccec5e04f

commit 54454ec7fbcbd043f7eafea03049e53ccec5e04f
Author: David Manouchehri <david@davidmanouchehri.com>
Date: Wed Feb 19 00:29:19 2020

Verify if the context is still available.

~~Bug: 1051748~~
Change-Id: I6bbef3ef50930048984593270fbe39a59a6d61f3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2053167
Reviewed-by: Shrek Shao <shrekshao@google.com>
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Kenneth Russell <kbr@chromium.org>
Auto-Submit: David Manouchehri <david@davidmanouchehri.com>
Cr-Commit-Position: refs/heads/master@{#742401}

[modify] https://crrev.com/54454ec7fbcbd043f7eafea03049e53ccec5e04f/third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc

Comment 20 by sheriffbot on Wed, Feb 19, 2020, 11:43 AM EST
Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 21 by kbr@chromium.org on Wed, Feb 19, 2020, 2:44 PM EST
Status: Fixed (was: Assigned)

We believe this is fixed with the above CL.

Comment 22 by da...@davidmanouchehri.com on Wed, Feb 19, 2020, 2:46 PM EST
I think this should have the Security_Impact-Stable label added back, not sure why ClusterFuzz removed it.

Comment 23 by kbr@chromium.org on Wed, Feb 19, 2020, 8:24 PM EST
Labels: Security_Impact-Stable

Comment 24 by ClusterFuzz on Thu, Feb 20, 2020, 5:15 AM EST
Status: Verified (was: Fixed)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5644307466878976 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=742396:742403

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

Comment 25 by sheriffbot on Thu, Feb 20, 2020, 12:24 PM EST
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 26 by natashapabrai@google.com on Mon, Feb 24, 2020, 2:12 PM EST
Labels: reward-topanel

Comment 27 by sheriffbot on Mon, Feb 24, 2020, 2:26 PM EST
Labels: Merge-Request-81

Requesting merge to beta M81 because latest trunk commit (742401) appears to be after beta branch point (737173).

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

Comment 28 by sheriffbot on Mon, Feb 24, 2020, 2:27 PM EST
Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: M81's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

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

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

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

Comment 29 by pbommana@google.com on Tue, Feb 25, 2020, 5:06 PM EST
Cc: adetaylor@chromium.org

+adetaylor@(Security TPM) for inputs.

shrekshao@google.com please provide the details w.r.t questions posted in comment#28 which would help us in approval process.

Comment 30 by shrekshao@google.com on Tue, Feb 25, 2020, 5:23 PM EST

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
The CL is landed on Feb 19 2020. which is within four weeks of beta rollout.
This is a minor tweak.
The bug is not release blocking though. Target-81 label is added by sheriff
2. Links to the CLs you are requesting to merge.
Commit: https://chromium.googlesource.com/chromium/src/+/54454ec7fbcbd043f7eafea03049e53ccec5e04f
Reviewed on: https://chromium-review.googlesource.com/c/chromium/src/+/2053167
3. Has the change landed and been verified on master/ToT?
Yes
4. Why are these changes required in this milestone after branch?
It's a defect that could lead to a tab/renderer crash. The fix is verified by clusterfuzz
5. Is this a new feature?
No
6. If it is a new feature, is it behind a flag using finch?
N/A

Comment 31 by adetaylor@chromium.org on Tue, Feb 25, 2020, 6:41 PM EST

Labels: -Merge-Review-81 Merge-Approved-81

Yes, please merge to M81 (branch: 4044).

Comment 32 by bugdroid on Tue, Feb 25, 2020, 9:29 PM EST

Labels: -merge-approved-81 merge-merged-81 merge-merged-4044

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/8a429ea726a967e02c5a57c2bf6819c3c39e1c24

commit 8a429ea726a967e02c5a57c2bf6819c3c39e1c24
Author: shrekshao <shrekshao@google.com>
Date: Wed Feb 26 02:27:24 2020

[M81 merge] Verify if the context is still available.

TBR=david@davidmanouchehri.com
(cherry picked from commit 54454ec7fbcbd043f7eafea03049e53ccec5e04f)

~~Bug: 1051748~~
Change-Id: I2806d3fcdcc54e7b9f3247893de49a5d88cb31b8
Reviewed-by: Shrek Shao <shrekshao@google.com>
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Kenneth Russell <kbr@chromium.org>
Auto-Submit: David Manouchehri <david@davidmanouchehri.com>
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2073150
Commit-Queue: Shrek Shao <shrekshao@google.com>
Cr-Commit-Position: refs/branch-heads/4044@{#484}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/8a429ea726a967e02c5a57c2bf6819c3c39e1c24/third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc

Comment 33 by natashapabrai@google.com on Wed, Feb 26, 2020, 7:20 PM EST

Labels: -reward-topanel reward-unpaid reward-8500

*** 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 34 by natashapabrai@google.com on Wed, Feb 26, 2020, 7:28 PM EST

Labels: -Security_Severity-Medium Security_Severity-High

Congrats the Panel decided to award $7,500 for this report and an additional $1,000 patch bonus. Nice one!

Comment 35 by natashapabrai@google.com on Tue, Mar 3, 2020, 11:42 AM EST

Labels: -reward-unpaid reward-inprocess

Comment 36 by da...@davidmanouchehri.com on Wed, Mar 4, 2020, 8:52 PM EST

Now I regret not providing patches for my previous tickets. =P

Could I have a CVE for this one too? =)

Comment 37 by adetaylor@chromium.org on Thu, Mar 5, 2020, 2:02 PM EST

This will get a CVE when it's released and credited in the release notes. Thanks for the report!

Comment 38 by mmoroz@google.com on Tue, Mar 10, 2020, 1:04 PM EDT

Labels: VulnerabilityAnalysis-Requested

shrekshao@, thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: https://forms.gle/VWKDUv9a8GXCCRWm7

Comment 39 by adetaylor@google.com on Fri, Mar 13, 2020, 1:44 PM EDT

Labels: Release-0-M81

Comment 40 by adetaylor@chromium.org on Fri, Mar 13, 2020, 2:30 PM EDT

Labels: CVE-2020-6422 CVE_description-missing

Comment 41 Deleted

Comment 42 by gov...@chromium.org on Mon, Mar 16, 2020, 2:49 AM EDT

Labels: -Merge-Approved-80 Merge-Review-80

Changing it back to Merge-Review-80 as we're hitting merge conflict.

Taking adetaylor@'s input. Can we just skip for M80?

Comment 43 by bugdroid on Mon, Mar 16, 2020, 2:28 PM EDT

Labels: merge-merged-3987_137

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/01360ded829865a6ffc3cf3c25b1f2a109fa87d7

commit 01360ded829865a6ffc3cf3c25b1f2a109fa87d7
Author: shrekshao <shrekshao@google.com>
Date: Mon Mar 16 18:25:33 2020

Verify if the context is still available.

Resolve conflict manually with git-drover

~~Bug: 1051748~~
Change-Id: I6bbef3ef509300489845932 70fbe39a59a6d61f3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2053167
Reviewed-by: Shrek Shao <shrekshao@google.com>
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Kenneth Russell <kbr@chromium.org>
Auto-Submit: David Manouchehri <david@davidmanouchehri.com>
Cr-Commit-Position: refs/heads/master@{#742401}
(cherry picked from commit 54454ec7fbcbd043f7eafea03049e53ccec5e04f)

TBR=kbr@chromium.org

Change-Id: I76fb4fea4a0f34b45ca425df353b36efe66f4708
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104990
Reviewed-by: Shrek Shao <shrekshao@google.com>
Commit-Queue: Shrek Shao <shrekshao@google.com>
Cr-Commit-Position: refs/branch-heads/3987_137@{#14}
Cr-Branched-From: 55c16ce255e7a7feca588abeb4f082026b35e1ef-refs/branch-heads/3987@{#989}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/01360ded829865a6ffc3cf3c25b1f2a109fa87d7/third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc

Comment 44 by gov...@chromium.org on Mon, Mar 16, 2020, 8:42 PM EDT

Labels: Merge-Approved-80

Approving merge to M80 branch 3987, please merge ASAP. Thank you.

Comment 45 by gov...@chromium.org on Mon, Mar 16, 2020, 10:36 PM EDT

Labels: -Merge-Review-80

Comment 46 by bugdroid on Tue, Mar 17, 2020, 12:06 AM EDT

Labels: -merge-approved-80 merge-merged-3987 merge-merged-80

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/7361a8e5073fdf9bf6b102991485efe59ce4bb23

commit 7361a8e5073fdf9bf6b102991485efe59ce4bb23
Author: shrekshao <shrekshao@google.com>
Date: Tue Mar 17 04:05:24 2020

[M80 merge] Verify if the context is still available.

~~Bug: 1051748~~
Change-Id: I6bbef3ef509300489845932 70fbe39a59a6d61f3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2053167
Reviewed-by: Shrek Shao <shrekshao@google.com>
Reviewed-by: Kenneth Russell <kbr@chromium.org>
Commit-Queue: Kenneth Russell <kbr@chromium.org>
Auto-Submit: David Manouchehri <david@davidmanouchehri.com>
Cr-Commit-Position: refs/heads/master@{#742401}
(cherry picked from commit 54454ec7fbcbd043f7eafea03049e53ccec5e04f)

TBR=kbr@chromium.org

Change-Id: I34b3b6db1f1668012ab7cfd6c787b6a3ba5fec72
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2106751
Reviewed-by: Shrek Shao <shrekshao@google.com>
Commit-Queue: Shrek Shao <shrekshao@google.com>
Cr-Commit-Position: refs/branch-heads/3987@{#1014}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/7361a8e5073fdf9bf6b102991485efe59ce4bb23/third_party/blink/renderer/modules/webgl/webgl_rendering_context_base.cc

Comment 47 by adetaylor@google.com on Tue, Mar 17, 2020, 11:17 AM EDT

Labels: -Release-0-M81 Release-5-M80

Comment 48 by gov...@chromium.org on Tue, Mar 17, 2020, 4:33 PM EDT

Cc: prashanthpola@chromium.org

Comment 49 by adetaylor@chromium.org on Thu, Mar 19, 2020, 6:30 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 50 by adetaylor@google.com on Wed, Mar 25, 2020, 3:31 PM EDT

Cc: achuith@chromium.org

Comment 51 by sheriffbot on Thu, May 28, 2020, 2:56 PM EDT

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