


☆ Starred by 3 users

Owner: fs...@chromium.org

CC: adetaylor@chromium.org
sheriffbot
adetaylor@google.com
fs...@chromium.org
 yiyix@chromium.org

Status: Fixed (Closed)

Components: Blink>Canvas

Modified: Jun 23, 2020

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac, Fuchsia

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
reward-2000
Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
Hotlist-Merge-Approved
M-80
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-80
merge-merged-4085
merge-merged-82
Release-0-M83
CVE-2020-6474

Issue 1059533: use-after-free in web_graphics_context_3d_provider_wrapper

Reported by cdsrc...@gmail.com on Sat, Mar 7, 2020, 4:59 AM EST

 Code

UserAgent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36

Steps to reproduce the problem:
1 Build latest chrome(82.0.4079.0) with asan.
2 ./chrome <http://127.0.0.1:8605/crash.html>
3 Close the entire browser after about 5 seconds.
4 Get UAF.

What is the expected behavior?

What went wrong?
==100464==ERROR: AddressSanitizer: heap-use-after-free on address 0x60700006fa08 at pc 0x55601ada4c83 bp 0x7ffed88b0230 sp 0x7ffed88b0228
READ of size 8 at 0x60700006fa08 thread T0 (chrome)
#0 0x55601ada4c82 in get ./././buildtools/third_party/libc++/trunk/include/memory:2606:19
#1 0x55601ada4c82 in ContextProvider ./././third_party/blink/renderer/platform/graphics/web_graphics_context_3d_provider_wrapper.h:43:30
#2 0x55601ada4c82 in blink::CanvasResourceProvider::EnsureSkiaCanvas() ./././third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc:1043:14
#3 0x55601ada5b9e in blink::CanvasResourceProvider::FlushCanvas() ./././third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc:1134:3
#4 0x55601e863ffd in FlushRecording ./././third_party/blink/renderer/modules/canvas/offscreencanvas2d/offscreen_canvas_rendering_context_2d.cc:126:32
#5 0x55601e863ffd in blink::OffscreenCanvasRenderingContext2D::FinalizeFrame()
./././third_party/blink/renderer/modules/canvas/offscreencanvas2d/offscreen_canvas_rendering_context_2d.cc:139:3
#6 0x55601e6cc59a in blink::BaseRenderingContext2D::getImageData(int, int, int, blink::ExceptionState&)
./././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1614:3
#7 0x55601e891648 in GetImageDataMethod ./gen/third_party/blink/renderer/bindings/modules/v8/v8_offscreen_canvas_rendering_context_2d.cc:1969:29
#8 0x55601e891648 in blink::V8OffscreenCanvasRenderingContext2D::GetImageDataMethodCallback(v8::FunctionCallbackInfo<v8::Value> const&)
./gen/third_party/blink/renderer/bindings/modules/v8/v8_offscreen_canvas_rendering_context_2d.cc:3059:3
#9 0x55600a684ff in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./././v8/src/api/api-arguments-inl.h:158:3
#10 0x55600a68cf4d in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) ./././v8/src/builtins/builtins-api.cc:111:36
#11 0x55600a68ae0d in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) ./././v8/src/builtins/builtins-api.cc:141:5
#12 0x55600c630217 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
#13 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#14 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#15 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#16 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#17 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#18 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#19 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#20 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#21 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#22 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#23 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#24 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#25 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0

[illegible]

[illegible]

```
#232 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#233 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#234 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#235 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#236 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#237 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#238 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#239 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#240 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#241 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#242 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#243 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#244 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#245 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#246 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#247 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#248 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#249 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#250 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#251 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#252 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#253 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#254 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#255 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#256 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#257 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#258 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#259 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
```

0x60700006fa08 is located 8 bytes inside of 80-byte region [0x60700006fa00,0x60700006fa50) freed by thread T0 (chrome) here:

```
#0 0x556004d36d4 in free /b/s/w/r/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_malloc_linux.cpp:123:3
#1 0x55601adb4392 in operator delete /././third_party/blink/renderer/platform/graphics/web_graphics_context_3d_provider_wrapper.h:22:3
#2 0x55601adb4392 in operator() /././buildtools/third_party/libc++/trunk/include/memory:2378:5
#3 0x55601adb4392 in reset /././buildtools/third_party/libc++/trunk/include/memory:2633:7
#4 0x55601adb4392 in operator= /././buildtools/third_party/libc++/trunk/include/memory:2591:5
#5 0x55601adb4392 in blink::SharedGpuContext::CreateContextProviderIfNeeded(bool)
./././third_party/blink/renderer/platform/graphics/gpu/shared_gpu_context.cc:102:29
#6 0x55601adb4f86 in blink::SharedGpuContext::ContextProviderWrapper() /././third_party/blink/renderer/platform/graphics/gpu/shared_gpu_context.cc:45:13
#7 0x55601afb04cf in blink::HTMLCanvasElement::ShouldAccelerate(blink::HTMLCanvasElement::AccelerationCriteria) const
./././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1071:7
#8 0x55601afb04cf in blink::HTMLCanvasElement::SetCanvas2DLayerBridgeInternal(std::__1::unique_ptr<blink::Canvas2DLayerBridge,
std::__1::default_delete<blink::Canvas2DLayerBridge> >) /././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1116:9
#9 0x55601afb1b70 in blink::HTMLCanvasElement::GetOrCreateCanvas2DLayerBridge() /././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1163:5
#10 0x55601e67ce41 in GetOrCreatePaintCanvas /././third_party/blink/renderer/modules/canvas/canvas2d/canvas_rendering_context_2d.cc:443:17
#11 0x55601e67ce41 in non-virtual thunk to blink::CanvasRenderingContext2D::GetOrCreatePaintCanvas()
./././third_party/blink/renderer/modules/canvas/canvas2d/canvas_rendering_context_2d.cc:0:0
#12 0x55601e6c3623 in blink::BaseRenderingContext2D::drawImage(blink::ScriptState*, blink::CanvasImageSource*, double, double, double, double, double, double,
double, double, blink::ExceptionState&) /././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1172:8
#13 0x55601e6c282e in blink::BaseRenderingContext2D::drawImage(blink::ScriptState*,
blink::CSSImageValueOrHTMLImageElementOrSVGImageElementOrHTMLVideoElementOrHTMLCanvasElementOrImageBitmapOrOffscreenCanvas const&, double,
double, blink::ExceptionState&) /././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1006:3
#14 0x55601e705d64 in DrawImage1Method /gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:1805:9
#15 0x55601e705d64 in DrawImageMethod /gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:1915:9
#16 0x55601e705d64 in blink::V8CanvasRenderingContext2D::DrawImageMethodCallback(v8::FunctionCallbackInfo<v8::Value> const&)
/gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:3165:3
#17 0x55600a68f4ff in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) /././v8/src/api/api-arguments-inl.h:158:3
#18 0x55600a6c8fd4 in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) /././v8/src/builtins/builtins-api.cc:111:36
#19 0x55600a68ae0d in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) /././v8/src/builtins/builtins-api.cc:141:5
#20 0x55600c630217 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
#21 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#22 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#23 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#24 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#25 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#26 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#27 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#28 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#29 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#30 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#31 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#32 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#33 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#34 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#35 0x55600c5bbc1e in Builtins_ArgumentsAdaptorTrampoline ??:0:0
#36 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
```

previously allocated by thread T0 (chrome) here:

```
#0 0x556004d3944 in malloc /b/s/w/r/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_malloc_linux.cpp:145:3
#1 0x556013418419 in PartitionAllocGenericFlags /././base/allocator/partition_allocator/partition_alloc.h:402:48
#2 0x556013418419 in Alloc /././base/allocator/partition_allocator/partition_alloc.h:437:10
#3 0x556013418419 in WTF::Partitions::FastMalloc(unsigned long, char const*) /././third_party/blink/renderer/platform/wtf/allocator/partitions.cc:230:33
#4 0x55601adb46b0 in operator new /././third_party/blink/renderer/platform/graphics/web_graphics_context_3d_provider_wrapper.h:22:3
#5 0x55601adb46b0 in make_unique<blink::WebGraphicsContext3DProviderWrapper, std::__1::unique_ptr<blink::WebGraphicsContext3DProvider,
std::__1::default_delete<blink::WebGraphicsContext3DProvider> > > /././buildtools/third_party/libc++/trunk/include/memory:3043:28
#6 0x55601adb46b0 in blink::SharedGpuContext::CreateContextProviderIfNeeded(bool)
./././third_party/blink/renderer/platform/graphics/gpu/shared_gpu_context.cc:122:11
#7 0x55601adb4f86 in blink::SharedGpuContext::ContextProviderWrapper() /././third_party/blink/renderer/platform/graphics/gpu/shared_gpu_context.cc:45:13
#8 0x55601afb04cf in blink::HTMLCanvasElement::ShouldAccelerate(blink::HTMLCanvasElement::AccelerationCriteria) const
./././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1071:7
#9 0x55601afb04cf in blink::HTMLCanvasElement::SetCanvas2DLayerBridgeInternal(std::__1::unique_ptr<blink::Canvas2DLayerBridge,
std::__1::default_delete<blink::Canvas2DLayerBridge> >) /././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1116:9
#10 0x55601afb1b70 in blink::HTMLCanvasElement::GetOrCreateCanvas2DLayerBridge()
./././third_party/blink/renderer/core/html/canvas/html_canvas_element.cc:1163:5
#11 0x55601e67ce41 in GetOrCreatePaintCanvas /././third_party/blink/renderer/modules/canvas/canvas2d/canvas_rendering_context_2d.cc:443:17
#12 0x55601e67ce41 in non-virtual thunk to blink::CanvasRenderingContext2D::GetOrCreatePaintCanvas()
./././third_party/blink/renderer/modules/canvas/canvas2d/canvas_rendering_context_2d.cc:0:0
#13 0x55601e6c3623 in blink::BaseRenderingContext2D::drawImage(blink::ScriptState*, blink::CanvasImageSource*, double, double, double, double, double, double,
double, double, blink::ExceptionState&) /././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1172:8
#14 0x55601e6c282e in blink::BaseRenderingContext2D::drawImage(blink::ScriptState*,
blink::CSSImageValueOrHTMLImageElementOrSVGImageElementOrHTMLVideoElementOrHTMLCanvasElementOrImageBitmapOrOffscreenCanvas const&, double,
```

```
double, blink::ExceptionState&) ./././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1006:3
#15 0x55601e705d64 in DrawImage1Method ./gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:1805:9
#16 0x55601e705d64 in DrawImageMethod ./gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:1915:9
#17 0x55601e705d64 in blink::V8CanvasRenderingContext2D::DrawImageMethodCallback(v8::FunctionCallbackInfo<v8::Value> const&)/
./gen/third_party/blink/renderer/bindings/modules/v8/v8_canvas_rendering_context_2d.cc:3165:3
#18 0x55600a68f4ff in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./././v8/src/api/api-arguments-inl.h:158:3
#19 0x55600a68cf4d in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) ./././v8/src/builtins/builtins-api.cc:111:36
#20 0x55600a68ae0d in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) ./././v8/src/builtins/builtins-api.cc:141:5
#21 0x55600c630217 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
#22 0x55600c5c2170 in Builtins_InterpreterEntryTrampoline ??:0:0
#23 0x55600c5bfc99 in Builtins_JSEntryTrampoline ??:0:0
#24 0x55600c5bfa97 in Builtins_JSEntry ??:0:0
#25 0x55600a91a4cc in Call ./././v8/src/execution/simulator.h:142:12
#26 0x55600a91a4cc in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous namespace)::InvokeParams const&)/
./././v8/src/execution/execution.cc:367:33
#27 0x55600a91945e in v8::internal::Execution::Call(v8::internal::Isolate*, v8::internal::Handle<v8::internal::Object>, v8::internal::Handle<v8::internal::Object>, int,
v8::internal::Handle<v8::internal::Object>*) ./././v8/src/execution/execution.cc:461:10
#28 0x55600a5349b6 in v8::Script::Run(v8::Local<v8::Context>) ./././v8/src/api/api.cc:2201:7
#29 0x556018e81e45 in blink::V8ScriptRunner::RunCompiledScript(v8::Isolate*, v8::Local<v8::Script>, blink::ExecutionContext*)
./././third_party/blink/renderer/bindings/core/v8/v8_script_runner.cc:358:22
#30 0x55601a4e8840 in blink::ScriptController::ExecuteScriptAndReturnValue(v8::Local<v8::Context>, blink::ScriptSourceCode const&, blink::KURL const&,
blink::SanitizeScriptErrors, blink::ScriptFetchOptions const&)/././third_party/blink/renderer/bindings/core/v8/script_controller.cc:132:20
#31 0x55601a4eb46a in blink::ScriptController::EvaluateScriptInMainWorld(blink::ScriptSourceCode const&, blink::KURL const&, blink::SanitizeScriptErrors,
blink::ScriptFetchOptions const&, blink::ScriptController::ExecuteScriptPolicy) ./././third_party/blink/renderer/bindings/core/v8/script_controller.cc:360:33
#32 0x55601a4ebe8e in blink::ScriptController::ExecuteScriptInMainWorld(blink::ScriptSourceCode const&, blink::KURL const&, blink::SanitizeScriptErrors,
blink::ScriptFetchOptions const&)/././third_party/blink/renderer/bindings/core/v8/script_controller.cc:325:3
#33 0x55601c82a239 in blink::PendingScript::ExecuteScriptBlockInternal(blink::Script*, blink::ScriptElementBase*, bool, bool, bool, base::TimeTicks, bool)
./././third_party/blink/renderer/core/script/pending_script.cc:267:13
#34 0x55601c829ca0 in blink::PendingScript::ExecuteScriptBlock(blink::KURL const&)/././third_party/blink/renderer/core/script/pending_script.cc:175:3
#35 0x55601c82ef08 in blink::ScriptLoader::PrepareScript(WTF::TextPosition const&, blink::ScriptLoader::LegacyTypeSupport)
./././third_party/blink/renderer/core/script/script_loader.cc:917:9
#36 0x55601c7c9f37 in blink::HTMLParserScriptRunner::ProcessScriptElementInternal(blink::Element*, WTF::TextPosition const&)/
./././third_party/blink/renderer/core/script/html_parser_script_runner.cc:610:20
#37 0x55601c7c9aa8 in blink::HTMLParserScriptRunner::ProcessScriptElement(blink::Element*, WTF::TextPosition const&)/
./././third_party/blink/renderer/core/script/html_parser_script_runner.cc:333:3
```

SUMMARY: AddressSanitizer: heap-use-after-free (/home/cowboy/chromium/src/out/chrome_asan_shared/chrome+0x1fc54c82)

Shadow bytes around the buggy address:

```
0x0c0e80005ef0: fd fd fd fd fa fa fa fa fa fa fa fa
0x0c0e80005f00: fa fa fa fa fa fa fd fd fd fd fd fd
0x0c0e80005f10: fd fd fa fa fa fd fd fd fd fd fd fa
0x0c0e80005f20: fa fa fa fa fd fd fd fd fd fd fa fa
0x0c0e80005f30: fa fa fd fd fd fd fd fd fd fd fa fa
=>0x0c0e80005f40: fd[fd]fd fd fd fd fd fd fa fa fa fa
0x0c0e80005f50: fa fa fa fa fa fa fa fa fa fd fd fd
0x0c0e80005f60: fd fd fd fd fa fa fa fa fd fd fd fd
0x0c0e80005f70: fd fd fd fa fa fa fd fd fd fd fd fd
0x0c0e80005f80: fd fa fa fa fd fd fd fd fd fd fd fd
0x0c0e80005f90: fa fa fa fa fa fa fa fa fa fa fa
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
Shadow gap: cc
==100464==ABORTING
```

Received signal 6

```
#0 0x5560040931bb in backtrace /b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/./sanitizer_common/sanitizer_common_interceptors.inc:4107:13
#1 0x55600e909474 in base::debug::CollectStackTrace(void**, unsigned long) ./././base/debug/stack_trace_posix.cc:840:39
#2 0x55600e6b5592 in StackTrace ./././base/debug/stack_trace.cc:206:12
#3 0x55600e6b5592 in base::debug::StackTrace::StackTrace() ./././base/debug/stack_trace.cc:203:28
#4 0x55600e907d98 in base::debug::(anonymous namespace)::StackDumpSignalHandler(int, siginfo_t*, void*) ./././base/debug/stack_trace_posix.cc:345:3
#5 0x7f9d57bb0890 in __funlockfile ???
#6 0x7f9d57bb0890 in ?? ???
#7 0x7f9d502d5e97 in __libc_signal_restore_set /build/glibc-OTsEL5/glibc-2.27/signal/./sysdeps/unix/sysv/linux/nptl-signals.h:80:0
#8 0x7f9d502d5e97 in raise /build/glibc-OTsEL5/glibc-2.27/signal/./sysdeps/unix/sysv/linux/raise.c:48:0
#9 0x7f9d502d7801 in abort /build/glibc-OTsEL5/glibc-2.27/stdlib/abort.c:79:0
#10 0x5560040e9785 in __sanitizer::Abort() /b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/sanitizer_common/sanitizer_posix_libcdep.cpp:155:3
#11 0x5560040e85d5 in __sanitizer::Die() /b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/sanitizer_common/sanitizer_termination.cpp:58:5
#12 0x5560040d774a in __asan::ScopedInErrorReport::~ScopedInErrorReport() /b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_report.cpp:186:7
#13 0x5560040d90ab in __asan::ReportGenericError(unsigned long, unsigned long, unsigned long, unsigned long, bool, unsigned long, unsigned int, bool)
/b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_report.cpp:474:1
#14 0x5560040d9988 in __asan_report_load8 /b/s/wlir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_rtl.cpp:120:1
#15 0x55601ada4c83 in get ./././buildtools/third_party/libc++/trunk/include/memory:2606:19
#16 0x55601ada4c83 in ContextProvider ./././third_party/blink/renderer/platform/graphics/web_graphics_context_3d_provider_wrapper.h:43:30
#17 0x55601ada4c83 in blink::CanvasResourceProvider::EnsureSkiaCanvas() ./././third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc:1043:14
#18 0x55601ada5b9f in blink::CanvasResourceProvider::FlushCanvas() ./././third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc:1134:3
#19 0x55601e863ffe in FlushRecording ./././third_party/blink/renderer/modules/canvas/offscreencanvas2d/offscreen_canvas_rendering_context_2d.cc:126:32
#20 0x55601e863ffe in blink::OffscreenCanvasRenderingContext2D::FinalizeFrame()
./././third_party/blink/renderer/modules/canvas/offscreencanvas2d/offscreen_canvas_rendering_context_2d.cc:139:3
#21 0x55601e6cc59b in blink::BaseRenderingContext2D::getImageData(int, int, int, int, blink::ExceptionState&)/
./././third_party/blink/renderer/modules/canvas/canvas2d/base_rendering_context_2d.cc:1614:3
#22 0x55601e891649 in GetImageDataMethod ./gen/third_party/blink/renderer/bindings/modules/v8/v8_offscreen_canvas_rendering_context_2d.cc:1969:29
#23 0x55601e891649 in blink::V8OffscreenCanvasRenderingContext2D::GetImageDataMethodCallback(v8::FunctionCallbackInfo<v8::Value> const&)/
./gen/third_party/blink/renderer/bindings/modules/v8/v8_offscreen_canvas_rendering_context_2d.cc:3059:3
#24 0x55600a68f500 in v8::internal::FunctionCallbackArguments::Call(v8::internal::CallHandlerInfo) ./././v8/src/api/api-arguments-inl.h:158:3
#25 0x55600a68cf4d in v8::internal::MaybeHandle<v8::internal::Object> v8::internal::(anonymous namespace)::HandleApiCallHelper<false>(v8::internal::Isolate*,
```

```
v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::HeapObject>, v8::internal::Handle<v8::internal::FunctionTemplateInfo>,
v8::internal::Handle<v8::internal::Object>, v8::internal::BuiltinArguments) J.J./v8/src/builtins/builtins-api.cc:111:36
#26 0x55600a68ae0e in v8::internal::Builtin_Impl_HandleApiCall(v8::internal::BuiltinArguments, v8::internal::Isolate*) J.J./v8/src/builtins/builtins-api.cc:141:5
#27 0x55600c630218 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_BuiltinExit ??:0:0
r8: 0000000000000000 r9: 00007ffed88af270 r10: 0000000000000008 r11: 0000000000000046
r12: 00007ffed88b0228 r13: 00007ffed88b0230 r14: 00007ffed88b01d0 r15: 0000556022a739c8
di: 0000000000000002 si: 00007ffed88af270 bp: 00007ffed88b0200 bx: 00005560229e1588
dx: 0000000000000000 ax: 0000000000000000 cx: 00007f9d502d5e97 sp: 00007ffed88af270
ip: 00007f9d502d5e97 efl: 0000000000000046 cgf: 002b000000000033 erf: 0000000000000000
trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]
Calling _exit(1). Core file will not be generated.
```

Did this work before? N/A

Chrome version: Chromium 82.0.4079.0 Channel: n/a
OS Version: 18.04
Flash Version:

[Deleted] poc.zip

Comment 1 by ClusterFuzz on Tue, Mar 10, 2020, 9:55 PM EDT
ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=6290462112546816>.

Comment 2 by ClusterFuzz on Tue, Mar 10, 2020, 10:37 PM EDT
Labels: Security_Impact-Stable
Testcase 6290462112546816 failed to reproduce the crash. Please inspect the program output at <https://clusterfuzz.com/testcase?key=6290462112546816>.

Comment 3 by mpdenton@google.com on Wed, Mar 11, 2020, 3:56 AM EDT
Cc: fs...@chromium.org
Haven't been able to reproduce this on my Linux machine. Which OS does this occur on?

This is also an odd bug since it appears to be accessing the free object through a WeakPtr. It seems to occur in offscreen canvas code, fserb@ can you take a look?

Comment 4 by tsepez@chromium.org on Wed, Mar 11, 2020, 12:33 PM EDT
Owner: fs...@chromium.org

Comment 5 by tsepez@chromium.org on Wed, Mar 11, 2020, 1:25 PM EDT
Labels: Security_Severity-High

Comment 6 by sheriffbot on Wed, Mar 11, 2020, 1:34 PM EDT
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 fs...@chromium.org on Wed, Mar 11, 2020, 1:35 PM EDT
Owner: yiyix@chromium.org
Components: Blink>Canvas

Comment 8 by sheriffbot on Wed, Mar 11, 2020, 2:41 PM EDT
Status: Assigned (was: Unconfirmed)

Comment 9 by cdsr...@gmail.com on Thu, Mar 12, 2020, 5:02 AM EDT
OS:Ubuntu 18.04
Chromium version 82.0.4084.0

I tested it in a more recent version. It cannot be reproduced with the above method.
Now need to add an extra launch switch, "--no-sandbox".

asan2.txt
37.9 KB View Download

Comment 10 by sheriffbot on Thu, Mar 12, 2020, 12:55 PM EDT
Labels: Target-80 M-80
Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 11 Deleted

Comment 12 by fs...@chromium.org on Mon, Mar 16, 2020, 10:31 AM EDT
Working on it.

Comment 13 by fs...@chromium.org on Mon, Mar 16, 2020, 10:49 AM EDT
fix under review.

Comment 14 by bugdroid on Mon, Mar 16, 2020, 3:54 PM EDT
The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src.git/+fb38622fe2ee22a7ba0f844b9c922c3bf41bc91>

commit fb38622fe2ee22a7ba0f844b9c922c3bf41bc91
Author: Fernando Serboncini <fserb@chromium.org>
Date: Mon Mar 16 19:53:28 2020

Check for ContextProviderWrapper before using it
ContextProviderWrapper is a weak pointer which may have disappeared.

Bug-1050533
Change-Id: Ibcc8a8a0b453d90757d2d210d04ba035f84d1268
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2105614>
Commit-Queue: Fernando Serboncini <fserb@chromium.org>
Commit-Queue: Yi Xu <yiyix@chromium.org>
Auto-Submit: Fernando Serboncini <fserb@chromium.org>

Reviewed-by: Yi Xu <yyix@chromium.org>
Cr-Commit-Position: refs/heads/master@{#750679}

[modify] https://crrev.com/ffb38622fe22a7ba0f844b9c922c3bf41bc91/third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc

Comment 15 by fs...@chromium.org on Mon, Mar 16, 2020, 4:00 PM EDT

Status: Fixed (was: Started)

gg

Comment 16 by fs...@chromium.org on Mon, Mar 16, 2020, 4:00 PM EDT

I'm guessing we don't need to merge this, as it's only repro-able with no-sandbox, but if someone from security wants to chime in, please do.

Comment 17 by mpdenton@google.com on Mon, Mar 16, 2020, 4:12 PM EDT

I'm a bit confused how we get a UAF. I thought WeakPtr::get() return a nullptr if the weak ptr was dead?

Also, do we know how this was occurring and how it was triggered? I'm not sure I'm qualified to answer whether this is triggerable without --no-sandbox. If it can only occur with the --no-sandbox flag then no need for a merge, and this perhaps shouldn't be tracked as a security bug.

Comment 18 by natashapabral@google.com on Mon, Mar 16, 2020, 6:43 PM EDT

Labels: reward-topanel

Comment 19 by sheriffbot on Tue, Mar 17, 2020, 2:00 PM EDT

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

Comment 20 by sheriffbot on Tue, Mar 17, 2020, 2:20 PM EDT

Labels: Merge-Request-81 Merge-Request-80

Requesting merge to stable M80 because latest trunk commit (750679) appears to be after stable branch point (722274).

Requesting merge to beta M81 because latest trunk commit (750679) appears to be after beta branch point (737173).

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

Comment 21 by sheriffbot on Tue, Mar 17, 2020, 2:23 PM EDT

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: Request affecting a post-stable build

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), bindusuvama@(iOS), geohsu@(ChromeOS), pbomma@(Desktop)

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

Comment 22 by adetaylor@google.com on Wed, Mar 18, 2020, 11:23 AM EDT

Labels: Merge-Request-82

Three branches active, three merge requests. Oh deary me.

Comment 23 by adetaylor@google.com on Wed, Mar 18, 2020, 11:36 AM EDT

mpdenton@ fserb@ I don't want to approve these merge requests until we understand it fully per #c16 and #c17. Please let me know!

Comment 24 by adetaylor@google.com on Wed, Mar 18, 2020, 11:36 AM EDT

Cc: adetaylor@chromium.org

Comment 25 by sheriffbot on Thu, Mar 19, 2020, 11:25 AM EDT

Labels: -Merge-Request-82 Hotlist-Merge-Approved Merge-Approved-82

Your change meets the bar and is auto-approved for M82. Please go ahead and merge the CL to branch 4085 (refs/branch-heads/4085) manually. Please contact milestone owner if you have questions.

Merge instructions: <https://www.chromium.org/developers/how-tos/drover>

Owners: govind@(Android), kariahda@(iOS), cindyb@(ChromeOS), Lakpamarthy@(Desktop)

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

Comment 26 by sheriffbot on Mon, Mar 23, 2020, 12:10 PM EDT

Cc: sheriffbot adetaylor@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 27 by bugdroid on Mon, Mar 23, 2020, 1:57 PM EDT

Labels: -merge-approved-82 merge-merged-4085 merge-merged-82

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+db37c4f9de2e9e8c0c3fc4e05df094a0b73f3481>

commit db37c4f9de2e9e8c0c3fc4e05df094a0b73f3481

Author: Fernando Serboncini <fserb@chromium.org>

Date: Mon Mar 23 17:56:33 2020

Check for ContextProviderWrapper before using it

ContextProviderWrapper is a weak pointer which may have disappeared.

(cherry picked from commit fbf38622fe22a7ba0f844b9c922c3bf41bc91)

~~Bug-408033~~

Change-Id: Ibcc8a8a0b453d90757d2d210d04ba035f84d1268
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2105614>
Commit-Queue: Fernando Serboncini <fserb@chromium.org>
Commit-Queue: Yi Xu <yiix@chromium.org>
Auto-Submit: Fernando Serboncini <fserb@chromium.org>
Reviewed-by: Yi Xu <yiix@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#750679}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2115758>
Reviewed-by: Fernando Serboncini <fserb@chromium.org>
Cr-Commit-Position: refs/branch-heads/4085@{#200}
Cr-Branched-From: 938fda43077d4622c5b88984608d6becd5ebbb82-refs/heads/master@{#749737}

[modify] https://crrev.com/db37cf4f9de2e9e8c0c3fc4e05df094a0b73f3481/third_party/blink/renderer/platform/graphics/canvas_resource_provider.cc

Comment 28 by adetaylor@chromium.org on Mon, Mar 23, 2020, 4:13 PM EDT

fserb@ please see [#c23](#). We'd like to get this moving into M81 and M80 but I'm concerned that there's still uncertainty. Obviously we merge into the currently active stable release only if we're totally sure of "everything" so I just want to make sure there is no remaining doubt.

Comment 29 by fs...@chromium.org on Mon, Mar 23, 2020, 5:03 PM EDT

I don't think we need to merge back.

Comment 30 by adetaylor@google.com on Mon, Mar 23, 2020, 5:27 PM EDT

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

Can you expand on that? Since March 16th your CL will have been visible in git with a description which indicates a UaF, and patch-gappers can often weaponize them within 5 days. As this was externally reported and might be findable using fuzzing. There's every chance that Chrome users are under attack from this bug right now. So I absolutely do think we need to merge back... but I don't want to approve merge to a current stable branch until we're certain what's going on. People get upset if I approve the merge of something which breaks the internet for 3 billion people.)

(Incidentally, adding more platforms on the assumption that this is a cross-platform bug. Please fix if not).

Comment 31 by fs...@chromium.org on Wed, Mar 25, 2020, 3:18 PM EDT

Our current understanding is: this bug doesn't repro without --no-sandbox.

The reason this happens even with the WeakPtr, is that the Wrapper is on the WeakPtr, but not the actual class, so we end up (somehow) in this situation where the Wrapper is valid (the class is still up), but the actual pointer that it wraps has been deleted. (Come to think of it, I think the CL may be wrong and we are testing the wrong pointer).

I don't fully understand why this happens only with no-sandbox, it could be because of some weird ordering we destroy objects.

If this is a no-sandbox only bug, I don't think it even should be High security.

Comment 32 by adetaylor@google.com on Wed, Mar 25, 2020, 3:21 PM EDT

Labels: -Security_Severity-High -Merge-Request-80 Security_Severity-Medium

OK. Thanks very much. Even with that uncertainty, then, I'll assume it does apply only in the --no-sandbox case and we won't merge this further.

Comment 33 by adetaylor@google.com on Wed, Mar 25, 2020, 3:21 PM EDT

Labels: -Merge-Review-81

Comment 34 by natashapabrai@google.com on Thu, Mar 26, 2020, 5:26 PM EDT

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 35 by natashapabrai@google.com on Thu, Mar 26, 2020, 5:49 PM EDT

Congrats! The Panel decided to award \$2,000 for this report!

Comment 36 by natashapabrai@google.com on Thu, Mar 26, 2020, 5:57 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 37 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT

Labels: Release-0-M83

Comment 38 by adetaylor@chromium.org on Mon, May 18, 2020, 11:58 AM EDT

Labels: CVE-2020-6474 CVE_description-missing

Comment 39 by adetaylor@chromium.org on Wed, May 20, 2020, 11:43 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 40 by sheriffbot on Tue, Jun 23, 2020, 3:01 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