Talos Vulnerability Report

TALOS-2021-1238

Webkit WebCore::GraphicsContext use-after-free vulnerability

JUNE 2, 2021

CVE NUMBER

CVE-2021-21779

Summary

A use-after-free vulnerability exists in the way Webkit's GraphicsContext handles certain events in WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. A victim must be tricked into visiting a malicious web page to trigger this vulnerability.

Tested Versions

Webkit WebKitGTK 2.30.4

Product URLs

https://webkit.org/

CVSSv3 Score

6.8 - CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:L

CWE

CWE-416 - Use After Free

Details

WebKit is an open-source web content engine for browsers and other applications.

The vulnerability lies in how WebKit handles function `fillText`. From documentation: `The CanvasRenderingContext2D method fillText() draws a text string at the specified coordinates, filling the string's characters with the current fillStyle. An optional parameter allows specifying a maximum width for the rendered text` The CanvasRenderingContext2D is created from HTMLCanvasElement by calling function `getContext('2d')`.

Canvas element itself is HTMLCanvasElement and posesses attributes called `width` and `height`. This vulnerability is due to `height` attribute.

```
1:  RETURN_IF_EXCEPTION(throwScope, encodedJSValue());
2:  if (UNLIKELY(impl.callTracingActive()))
3:      CallTracer::recordCanvasAction(impl, "fillText"_s, { text, x, y, maxWidth });
4:  throwScope.release();
5:  impl.fillText(WTFMove(text), WTFMove(x), WTFMove(y), WTFMove(maxWidth));
6:  return JSValue::encode(jsUndefined());
```

At line 5 above, Webkit takes `text` as the 1st argument to fillText function, while 2nd and 3rd arguments are intigers `18428` and `20441` respectively.

Then code execution proceeds to method `CanvasRenderingContext2D::drawTextInternal`:

```
1:  void CanvasRenderingContext2D::drawTextInternal(const String& text, float x, float y, bool fill, Optional<float> maxWidth)
2:  {
3:  if (RuntimeEnabledFeatures::sharedFeatures().webAPIStatisticsEnabled())
4:      ResourceLoadObserver::shared().logCanvasWriteOrMeasure(this->canvas().document(), text);
5:
6:  if (!canDrawTextWithParams(x, y, fill, maxWidth))
7:      return;
8:
9:  String normalizedText = text;
10:  normalizeSpaces(normalizedText);
11:
12:  const RenderStyle* computedStyle;
13:  auto direction = toTextDirection(state().direction, &computedStyle);
14:  bool override = computedStyle ? isOverride(computedStyle->unicodeBidi()) : false;
15:
16:  TextRun textRun(normalizedText, 0, 0, AllowRightExpansion, direction, override, true);
17:  drawTextUnchecked(textRun, x, y, fill, maxWidth);
18:  }
```

At line 6, function checks if the passed width and height are within range.

```
1:  bool CanvasRenderingContext2DBase::canDrawTextWithParams(float x, float y, bool fill, Optional<float> maxWidth)
2:  {
3:      auto* c = drawingContext();
4:      if (!c)
5:          return false;
6:      if (!this->fontProxy()->realized())
7:          return false;
8:      if (!state().hasInvertibleTransform)
9:          return false;
10:      if (!std::isfinite(x) | !std::isfinite(y))
11:          return false;
12:      if (maxWidth && (!std::isfinite(maxWidth.value()) || maxWidth.value() <= 0))
13:          return false;
14:
15:      // If gradient size is zero, nothing would be painted.
16:      auto gradient = c->strokeGradient();
17:      if (!fill && gradient && gradient->isZeroSize())
18:          return false;
19:
20:      gradient = c->fillGradient();
21:      if (fill && gradient && gradient->isZeroSize())
22:          return false;
23:
24:      return true;
25:  }
26:
```

At line 3 an `HTMLCanvasElement` object is retrieved with `WebCore::CanvasBase` and `m_size` that has default values of `m_width` as `300` and `m_height` as `150`. Then the execution of line 6 proceeds to:

```
1:  auto CanvasRenderingContext2D::fontProxy() -> const FontProxy* {
2:      auto& canvas = downcast<HTMLCanvasElement>(canvasBase());
3:      canvas.document().updateStyleIfNeeded();
4:      if (!state().font.realized())
5:          setFont(state().unparsedFont);
6:      return &state().font;
7:  }
```

At line 2, a `HTMLCanvasElement` object is checked for any changes made in the background and the new `m_height` is set to value `87` according to the execution of `event_change_height`. At this point, the previous allocation is made with old height value (`old_m_height` of 150 minus `m_height` of 87 equals `63`). Afterwards, at line 20, a call to `fillGradient()` tries to read memory from old memory ranges which are now freed due to changes made when function `canvas.document().updateStyleIfNeeded();` was executed. This constitutes a use after free condition.

With proper memory layout control and heap grooming, an attacker would be able to take control of the erroneous memory reuse which could lead to information leak and possibly further memory corruption.

Crash Information

```
==76078==ERROR: AddressSanitizer: heap-use-after-free on address 0x6110000c8550 at pc 0x0002aacb31d7 bp 0x7ffeeb476b70 sp 0x7ffeeb476b68
READ of size 8 at 0x6110000c8550 thread T0
==76078==WARNING: invalid path to external symbolizer!
==76078==WARNING: Failed to use and restart external symbolizer!
    #0 0x2aacb31d6 in WTF::RefPtr<WebCore::Gradient, WTF::RawPtrTraits<WebCore::Gradient>, WTF::DefaultRefDerefTraits<WebCore::Gradient>
>::get() const+0x26 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d331d6)
    #1 0x2aac9f7ec in WebCore::GraphicsContext::strokeGradient() const+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d1f7ec)
    #2 0x2aac964a4 in WebCore::CanvasRenderingContext2DBase::canDrawTextWithParams(float, float, bool, WTF::Optional<float>)+0x134
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d164a4)
    #3 0x2aac9531f in WebCore::CanvasRenderingContext2D::drawTextInternal(WTF::String const&, float, float, bool,
WTF::Optional<float>)+0x17f (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d1531f)
    #4 0x2aac95140 in WebCore::CanvasRenderingContext2D::fillText(WTF::String const&, float, float, WTF::Optional<float>)+0xe0
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d15140)
    #5 0x2a76551bf in WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillTextBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSCanvasRenderingContext2D*)+0x50f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x6d51bf)
    #6 0x2a7654c0b in long long WebCore::IDLOperation<WebCore::JSCanvasRenderingContext2D>::call<&
(WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillTextBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSCanvasRenderingContext2D*)), (WebCore::CastedThisErrorBehavior)0>(JSC::JSGlobalObject&, JSC::CallFrame&, char const*)+0xfb
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x6d4c0b)
    #7 0x2a760de38 in WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillText(JSC::JSGlobalObject*, JSC::CallFrame*)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x68de38)
    #8 0x407929c011d7  (<unknown module>)
    #9 0x2c74efc55 in llint_entry+0x1a6fd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0xbc3c55)
    #10 0x2c74efc55 in llint_entry+0x1a6fd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0xbc3c55)
    #11 0x2c74d5358 in vmEntryToJavaScript+0xd7
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0xba9358)
    #12 0x2c8c4b930 in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue, JSC::ArgList
const&)+0x5e0 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x231f930)
    #13 0x2c92fcf44 in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&)+0x64
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x29d0f44)
    #14 0x2c92fd03f in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&,
WTF::NakedPtr<JSC::Exception>&)+0xdf
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x29d103f)
    #15 0x2c92fd3fb in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&)+0x10b
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x29d13fb)
    #16 0x2a9d69f98 in WebCore::JSExecState::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&)+0xe8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x2de9f98)
    #17 0x2a9d94698 in WebCore::JSEventListener::handleEvent(WebCore::ScriptExecutionContext&, WebCore::Event&)+0xa78
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x2e14698)
    #18 0x2aa5ecaa2 in WebCore::EventTarget::innerInvokeEventListeners(WebCore::Event&,
WTF::Vector<WTF::RefPtr<WebCore::RegisteredEventListener, WTF::RawPtrTraits<WebCore::RegisteredEventListener>,
WTF::DefaultRefDerefTraits<WebCore::RegisteredEventListener> >, 1ul, WTF::CrashOnOverflow, 16ul, WTF::FastMalloc>,
WebCore::EventTarget::EventInvokePhase)+0x522
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x366caa2)
    #19 0x2aa5e78f2 in WebCore::EventTarget::fireEventListeners(WebCore::Event&, WebCore::EventTarget::EventInvokePhase)+0x1b2
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x36678f2)
    #20 0x2ab4f60e2 in WebCore::DOMWindow::dispatchEvent(WebCore::Event&, WebCore::EventTarget*)+0x2b2
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x45760e2)
    #21 0x2ab507885 in WebCore::DOMWindow::dispatchLoadEvent()+0x225
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4587885)
    #22 0x2aa4b0005 in WebCore::Document::dispatchWindowLoadEvent()+0x55
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3530005)
    #23 0x2aa4afac2 in WebCore::Document::implicitClose()+0x2e2
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x352fac2)
    #24 0x2ab31e178 in WebCore::FrameLoader::checkCallImplicitClose()+0xd8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x439e178)
    #25 0x2ab31d752 in WebCore::FrameLoader::checkCompleted()+0x2b2
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x439d752)
    #26 0x2ab319d48 in WebCore::FrameLoader::finishedParsing()+0x1b8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4399d48)
    #27 0x2aa4ce2a2 in WebCore::Document::finishedParsing()+0x252
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x354e2a2)
    #28 0x2aadb1414 in WebCore::HTMLConstructionSite::finishedParsing()+0x24
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e31414)
    #29 0x2aae12c9d in WebCore::HTMLTreeBuilder::finished()+0x1d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e92c9d)
    #30 0x2aadb9d37 in WebCore::HTMLDocumentParser::end()+0x17
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e39d37)
    #31 0x2aadb7678 in WebCore::HTMLDocumentParser::attemptToRunDeferredScriptsAndEnd()+0x38
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e37678)
    #32 0x2aadb754a in WebCore::HTMLDocumentParser::prepareToStopParsing()+0x10a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e3754a)
    #33 0x2aadb9d7f in WebCore::HTMLDocumentParser::attemptToEnd()+0x3f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e39d7f)
    #34 0x2aadb9e59 in WebCore::HTMLDocumentParser::finish()+0x29
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e39e59)
    #35 0x2ab2eb700 in WebCore::DocumentWriter::end()+0x1a0
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x436b700)
    #36 0x2ab29cdec in WebCore::DocumentLoader::finishedLoading()+0x2dc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x431cdec)
    #37 0x2ab29c769 in WebCore::DocumentLoader::notifyFinished(WebCore::CachedResource&, WebCore::NetworkLoadMetrics const&)+0x2c9
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x431c769)
    #38 0x2ab45ab8f in WebCore::CachedResource::checkNotify(WebCore::NetworkLoadMetrics const&)+0x17f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x44dab8f)
    #39 0x2ab4551be in WebCore::CachedResource::finishLoading(WebCore::SharedBuffer*, WebCore::NetworkLoadMetrics const&)+0x4e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x44d51be)
    #40 0x2ab456a58 in WebCore::CachedRawResource::finishLoading(WebCore::SharedBuffer*, WebCore::NetworkLoadMetrics const&)+0x258
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x44d6a58)
    #41 0x2ab3d1d12 in WebCore::SubresourceLoader::didFinishLoading(WebCore::NetworkLoadMetrics const&)+0x732
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4451d12)
    #42 0x299f930b6 in WebKit::WebResourceLoader::didFinishResourceLoad(WebCore::NetworkLoadMetrics const&)+0x286
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x1f930b6)
    #43 0x29a6521b1 in void IPC::callMemberFunctionImpl<WebKit::WebResourceLoader, void (WebKit::WebResourceLoader::*)
(WebCore::NetworkLoadMetrics const&), std::__1::tuple<WebCore::NetworkLoadMetrics>, 0ul>(WebKit::WebResourceLoader*, void
(WebKit::WebResourceLoader::*)(WebCore::NetworkLoadMetrics const&), std::__1::tuple<WebCore::NetworkLoadMetrics>&&,
std::__1::integer_sequence<unsigned long, 0ul>)+0x61
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x26521b1)
    #44 0x29a652108 in void IPC::callMemberFunction<WebKit::WebResourceLoader, void (WebKit::WebResourceLoader::*)
(WebCore::NetworkLoadMetrics const&), std::__1::tuple<WebCore::NetworkLoadMetrics>, std::__1::integer_sequence<unsigned long, 0ul> >
(std::__1::tuple<WebCore::NetworkLoadMetrics>&&, WebKit::WebResourceLoader*, void (WebKit::WebResourceLoader::*)(WebCore::NetworkLoadMetrics
const&))+0x28 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x2652108)
    #45 0x29a64f816 in void IPC::handleMessage<Messages::WebResourceLoader::DidFinishResourceLoad, WebKit::WebResourceLoader, void
(WebKit::WebResourceLoader::*)(WebCore::NetworkLoadMetrics const&)>(IPC::Decoder&, WebKit::WebResourceLoader*, void
(WebKit::WebResourceLoader::*)(WebCore::NetworkLoadMetrics const&))+0x146
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x264f816)
    #46 0x29a64ee23 in WebKit::WebResourceLoader::didReceiveWebResourceLoaderMessage(IPC::Connection&, IPC::Decoder&)+0x1a3
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x264ee23)
```

```
    #47 0x299f7f9aa in WebKit::NetworkProcessConnection::didReceiveMessage(IPC::Connection&, IPC::Decoder&)+0xfa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x1f7f9aa)
    #48 0x2980969e3 in IPC::Connection::dispatchMessage(IPC::Decoder&)+0x293
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x969e3)
    #49 0x298098327 in IPC::Connection::dispatchMessage(std::__1::unique_ptr<IPC::Decoder, std::__1::default_delete<IPC::Decoder> >)+0x167
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x98327)
    #50 0x298098e56 in IPC::Connection::dispatchOneIncomingMessage()+0x196
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x98e56)
    #51 0x2980b7345 in IPC::Connection::enqueueIncomingMessage(std::__1::unique_ptr<IPC::Decoder, std::__1::default_delete<IPC::Decoder>
>)::$_8::operator()()+0x35 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0xb7345)
    #52 0x2980b72ac in WTF::Detail::CallableWrapper<IPC::Connection::enqueueIncomingMessage(std::__1::unique_ptr<IPC::Decoder,
std::__1::default_delete<IPC::Decoder> >)::$_8, void>::call()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0xb72ac)
    #53 0x2c696354e in WTF::Function<void ()>::operator()() const+0x3e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x3754e)
    #54 0x2c69f8868 in WTF::RunLoop::performWork()+0x228
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0xcc868)
    #55 0x2c69fbc35 in WTF::RunLoop::performWork(void*)+0xb5
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0xcfc35)
    #56 0x7fff2041d9fb in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x819fb)
    #57 0x7fff2041d963 in __CFRunLoopDoSource0+0xb3
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x81963)
    #58 0x7fff2041d6de in __CFRunLoopDoSources0+0xf7
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x816de)
    #59 0x7fff2041c110 in __CFRunLoopRun+0x379
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x80110)
    #60 0x7fff2041b6bd in CFRunLoopRunSpecific+0x232
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x7f6bd)
    #61 0x7fff211a5fa0 in -[NSRunLoop(NSRunLoop) runMode:beforeDate:]+0xd3
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0x5ffa0)
    #62 0x7fff21234383 in -[NSRunLoop(NSRunLoop) run]+0x4b
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0xee383)
    #63 0x7fff200753dc in _xpc_objc_main+0x338 (/usr/lib/system/libxpc.dylib:x86_64+0x153dc)
    #64 0x7fff20074e64 in xpc_main+0x1b4 (/usr/lib/system/libxpc.dylib:x86_64+0x14e64)
    #65 0x298e40a7f in WebKit::XPCServiceMain(int, char const**)+0x47f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0xe40a7f)
    #66 0x29a6f1f48 in WKXPCServiceMain+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x26f1f48)
    #67 0x104787e18 in main+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent.Development:x86_64+0
x100003e18)
    #68 0x7fff20340630 in start+0x0 (/usr/lib/system/libdyld.dylib:x86_64+0x15630)

0x6110000c8550 is located 16 bytes inside of 240-byte region [0x6110000c8540,0x6110000c8630)
freed by thread T0 here:
    #0 0x2a52a9dd6 in __sanitizer_mz_free+0x86
(/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/lib/clang/12.0.0/lib/darwin/libclang_rt.asan_osx_dynamic
.dylib:x86_64h+0x49dd6)
    #1 0x2c6afe9d4 in bmalloc::DebugHeap::free(void*)+0x24
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d29d4)
    #2 0x2c6afc548 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)+0x68
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d0548)
    #3 0x2c69811dd in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*)+0x7d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x551dd)
    #4 0x2c6980650 in bmalloc::api::free(void*, bmalloc::HeapKind)+0x10
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54650)
    #5 0x2c698063a in WTF::fastFree(void*)+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x5463a)
    #6 0x2a8f35188 in WebCore::GraphicsContext::operator delete(void*)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb5188)
    #7 0x2a8f38cda in std::__1::default_delete<WebCore::GraphicsContext>::operator()(WebCore::GraphicsContext*) const+0x1a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb8cda)
    #8 0x2a8f38c8c in std::__1::unique_ptr<WebCore::GraphicsContext, std::__1::default_delete<WebCore::GraphicsContext>
>::reset(WebCore::GraphicsContext*)+0x3c (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb8c8c)
    #9 0x2a8f38c4a in std::__1::unique_ptr<WebCore::GraphicsContext, std::__1::default_delete<WebCore::GraphicsContext> >::~unique_ptr()+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb8c4a)
    #10 0x2a8f2e338 in std::__1::unique_ptr<WebCore::GraphicsContext, std::__1::default_delete<WebCore::GraphicsContext>
>::~unique_ptr()+0x8 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fae338)
    #11 0x2a8f2e603 in WebCore::IOSurface::~IOSurface()+0x23
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fae603)
    #12 0x2a8f2e628 in WebCore::IOSurface::~IOSurface()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fae628)
    #13 0x2abb62082 in std::__1::default_delete<WebCore::IOSurface>::operator()(WebCore::IOSurface*) const+0x12
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4be2082)
    #14 0x2abb6204c in std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface>
>::reset(WebCore::IOSurface*)+0x3c (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4be204c)
    #15 0x2abb62008 in std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4be2008)
    #16 0x2abb513f8 in std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd13f8)
    #17 0x2abb5aa74 in WebCore::ImageBufferIOSurfaceBackend::~ImageBufferIOSurfaceBackend()+0x34
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bdaa74)
    #18 0x2abb58c08 in WebCore::ImageBufferIOSurfaceBackend::~ImageBufferIOSurfaceBackend()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd8c08)
    #19 0x2abb58c1d in WebCore::ImageBufferIOSurfaceBackend::~ImageBufferIOSurfaceBackend()+0xd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd8c1d)
    #20 0x2aba19749 in std::__1::default_delete<WebCore::ImageBufferIOSurfaceBackend>::operator()(WebCore::ImageBufferIOSurfaceBackend*)
const+0x39 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a99749)
    #21 0x2aba196ec in std::__1::unique_ptr<WebCore::ImageBufferIOSurfaceBackend,
std::__1::default_delete<WebCore::ImageBufferIOSurfaceBackend> >::reset(WebCore::ImageBufferIOSurfaceBackend*)+0x3c
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a996ec)
    #22 0x2aba199aa in std::__1::unique_ptr<WebCore::ImageBufferIOSurfaceBackend,
std::__1::default_delete<WebCore::ImageBufferIOSurfaceBackend> >::~unique_ptr()+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a999aa)
    #23 0x2aba16758 in std::__1::unique_ptr<WebCore::ImageBufferIOSurfaceBackend,
std::__1::default_delete<WebCore::ImageBufferIOSurfaceBackend> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a96758)
    #24 0x2aba19224 in WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend>::~ConcreteImageBuffer()+0x34
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a99224)
    #25 0x2aba18cf8 in WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend>::~ConcreteImageBuffer()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a98cf8)
    #26 0x2aba18d0d in WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend>::~ConcreteImageBuffer()+0xd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a98d0d)
    #27 0x2a7f26a89 in std::__1::default_delete<WebCore::ImageBuffer>::operator()(WebCore::ImageBuffer*) const+0x39
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0xfa6a89)
    #28 0x2a7f26a3d in WTF::RefCounted<WebCore::ImageBuffer, std::__1::default_delete<WebCore::ImageBuffer> >::deref() const+0x1d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0xfa6a3d)
    #29 0x2aaa2460d in WebCore::HTMLCanvasElement::setSurfaceSize(WebCore::IntSize const&)+0x12d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3aa460d)

previously allocated by thread T0 here:
    #0 0x2a52a99dd in __sanitizer_mz_malloc+0x9d
(/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/lib/clang/12.0.0/lib/darwin/libclang_rt.asan_osx_dynamic
.dylib:x86_64h+0x499dd)
    #1 0x7fff20165dfd in _malloc_zone_malloc+0x75 (/usr/lib/system/libsystem_malloc.dylib:x86_64+0x1bdfd)
    #2 0x2c6afe8e8 in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)+0x28
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d28e8)
```

```
    #3 0x2c6afc290 in bmalloc::Cache::allocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)+0x70
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d0290)
    #4 0x2c6980d0d in bmalloc::Cache::allocate(bmalloc::HeapKind, unsigned long)+0x7d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54d0d)
    #5 0x2c6980440 in bmalloc::api::malloc(unsigned long, bmalloc::HeapKind)+0x10
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54440)
    #6 0x2c69801ca in WTF::fastMalloc(unsigned long)+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x541ca)
    #7 0x2a8f35178 in WebCore::GraphicsContext::operator new(unsigned long)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb5178)
    #8 0x2a8f350e9 in std::__1::__unique_if<WebCore::GraphicsContext>::__unique_single std::__1::make_unique<WebCore::GraphicsContext,
CGContext*>(CGContext*&&)+0x19 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1fb50e9)
    #9 0x2a8f2ef0a in WebCore::IOSurface::ensureGraphicsContext()+0x10a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1faef0a)
    #10 0x2abb57cf7 in WebCore::ImageBufferIOSurfaceBackend::context() const+0x27
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd7cf7)
    #11 0x2abb52f42 in WebCore::ImageBufferCGBackend::setupContext() const+0xe2
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd2f42)
    #12 0x2abb57c83 in WebCore::ImageBufferIOSurfaceBackend::ImageBufferIOSurfaceBackend(WebCore::ImageBufferBackend::Parameters const&,
std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> >&&)+0x93
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd7c83)
    #13 0x2abb57cc8 in WebCore::ImageBufferIOSurfaceBackend::ImageBufferIOSurfaceBackend(WebCore::ImageBufferBackend::Parameters const&,
std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> >&&)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd7cc8)
    #14 0x2abb5a7a1 in std::__1::__unique_if<WebCore::ImageBufferIOSurfaceBackend>::__unique_single
std::__1::make_unique<WebCore::ImageBufferIOSurfaceBackend, WebCore::ImageBufferBackend::Parameters const&,
std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> > >(WebCore::ImageBufferBackend::Parameters const&,
std::__1::unique_ptr<WebCore::IOSurface, std::__1::default_delete<WebCore::IOSurface> >&&)+0x41
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bda7a1)
    #15 0x2abb578d7 in WebCore::ImageBufferIOSurfaceBackend::create(WebCore::ImageBufferBackend::Parameters const&, CGColorSpace*,
WebCore::HostWindow const*)+0x327 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd78d7)
    #16 0x2abb57bca in WebCore::ImageBufferIOSurfaceBackend::create(WebCore::ImageBufferBackend::Parameters const&, WebCore::HostWindow
const*)+0x4a (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4bd7bca)
    #17 0x2aba0b0b4 in WTF::RefPtr<WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend>,
WTF::RawPtrTraits<WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend> >,
WTF::DefaultRefDerefTraits<WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend> > >
WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend>::create<WebCore::ConcreteImageBuffer<WebCore::ImageBufferIOSurfaceBackend
> >(WebCore::FloatSize const&, float, WebCore::ColorSpace, WebCore::PixelFormat, WebCore::HostWindow const*)+0x184
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a8b0b4)
    #18 0x2aba0ae40 in WebCore::ImageBuffer::create(WebCore::FloatSize const&, WebCore::RenderingMode, float, WebCore::ColorSpace,
WebCore::PixelFormat, WebCore::HostWindow const*)+0x110
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a8ae40)
    #19 0x2aba0a992 in WebCore::ImageBuffer::create(WebCore::FloatSize const&, WebCore::RenderingMode, WebCore::ShouldUseDisplayList,
WebCore::RenderingPurpose, float, WebCore::ColorSpace, WebCore::PixelFormat, WebCore::HostWindow const*)+0x292
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4a8a992)
    #20 0x2aaa2741d in WebCore::HTMLCanvasElement::createImageBuffer() const+0x4bd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3aa741d)
    #21 0x2aa99b826 in WebCore::CanvasBase::buffer() const+0x66
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3a1b826)
    #22 0x2aa99b70d in WebCore::CanvasBase::drawingContext() const+0xbd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3a1b70d)
    #23 0x2aac943ed in WebCore::CanvasRenderingContext2DBase::drawingContext() const+0xfd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d143ed)
    #24 0x2aac96395 in WebCore::CanvasRenderingContext2DBase::canDrawTextWithParams(float, float, bool, WTF::Optional<float>)+0x25
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d16395)
    #25 0x2aac9531f in WebCore::CanvasRenderingContext2D::drawTextInternal(WTF::String const&, float, float, bool,
WTF::Optional<float>)+0x17f (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d1531f)
    #26 0x2aac95140 in WebCore::CanvasRenderingContext2D::fillText(WTF::String const&, float, float, WTF::Optional<float>)+0xe0
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d15140)
    #27 0x2a76551bf in WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillTextBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSCanvasRenderingContext2D*)+0x50f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x6d51bf)
    #28 0x2a7654c0b in long long WebCore::IDLOperation<WebCore::JSCanvasRenderingContext2D>::call<&
(WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillTextBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSCanvasRenderingContext2D*)), (WebCore::CastedThisErrorBehavior)0>(JSC::JSGlobalObject&, JSC::CallFrame&, char const*)+0xfb
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x6d4c0b)
    #29 0x2a760de38 in WebCore::jsCanvasRenderingContext2DPrototypeFunction_fillText(JSC::JSGlobalObject*, JSC::CallFrame*)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x68de38)

SUMMARY: AddressSanitizer: heap-use-after-free
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3d331d6) in WTF::RefPtr<WebCore::Gradient,
WTF::RawPtrTraits<WebCore::Gradient>, WTF::DefaultRefDerefTraits<WebCore::Gradient> >::get() const+0x26
Shadow bytes around the buggy address:
  0x1c2200019050: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x1c2200019060: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2200019070: fd fd fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c2200019080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x1c2200019090: 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa fa
=>0x1c22000190a0: fa fa fa fa fa fa fa fa fd fd[fd]fd fd fd fd fd
  0x1c22000190b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c22000190c0: fd fd fd fd fd fd fa fa fa fa fa fa fa fa fa fa
  0x1c22000190d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c22000190e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c22000190f0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==76078==ABORTING
```

Timeline

2021-02-02 - Vendor Disclosure

2021-05-25 - Vendor Patched

2021-06-02 - Public Release

CREDIT

Discovered by Marcin Towalski of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT

TALOS-2021-1246

NEXT REPORT

TALOS-2021-1258