Talos Vulnerability Report

TALOS-2020-1172

Webkit AudioSourceProviderGStreamer use-after-free vulnerability

MARCH 3, 2020

CVE NUMBER

CVE-2020-13558

Summary

A code execution vulnerability exists in the AudioSourceProviderGStreamer functionality of Webkit WebKitGTK 2.30.1. A specially crafted web page can lead to a use after free.

Tested Versions

Webkit WebKitGTK 2.30.1

Product URLs

https://webkit.org/

CVSSv3 Score

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

CWE

CWE-416 - Use After Free

Details

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

The vulnerabiliy is related with one of the WebAudio API interface `AudioSourceProviderGStreamer/MediaElementAudioSourceNode`, being more precise, the way its handled during its internal notification mechanism. A malicious web page can lead to a use-after-free vulnerability and remote code execution.

To understand the vulnerability let us analyze some parts of the poc.html file. First we need to create necessary WebAudio nodes :

```
Line 55         //choose destination nodes
Line 56         dst = new OfflineAudioContext({ numberOfChannels: 2, length: 44100 * 40, sampleRate: 44100,});
Line 58
Line 59         //choose source
Line 60         dst.createOscillator();
Line 62
Line 63         dst.onstatechange = eventhandler5; //OfflineAudioContext
Line 64
Line 65         console.log("OfflineAudioContext::startRendering");
Line 66         dst.startRendering();
```

After we run the poc in the Minibrowser we can observe that `eventhandler5` is executed 2 times:

```
Line 1          Start fuzzing
Line 2          OfflineAudioContext::startRendering
Line 3          eventhandler5
Line 4          =============
Line 5          event type :  statechange
Line 6          OfflineAudioContext.state :  running
Line 7             audioElement.load();
Line 8             audioCtx.createMediaElementSource( audioElement );
Line 9             setInterval(eventhandler4,53);
Line 10         eventhandler5
Line 11         =============
Line 12         event type :  statechange
Line 13         OfflineAudioContext.state :  closed
Line 14            audioElement.load();
Line 15         InvalidStateError: Media element is already associated with an audio source node
Line 16            setInterval(eventhandler4,53);
```

Each time there is an attempt to create a `MediaElementAudioSourceNode` (`line 8`) but that kind of node can be created just one time and that's why the second attempt ends up with an exception (`line 15`). Based on the log output we can observe that created `MediaElementAudioSourceNode` object is not assigned to any variable. Its allocation is clearly visible in asan output:

```
previously allocated by thread T0 here:
        #0 0x494bdd in malloc (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x494bdd)
        #1 0x7f33b9382cfb in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/DebugHeap.cpp:98:20
        #2 0x7f33b937f018 in bmalloc::Cache::tryAllocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/Cache.cpp:57:27
        #3 0x7f33c41265be in bmalloc::Cache::tryAllocate(bmalloc::HeapKind, unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:73:16
        #4 0x7f33c412614a in bmalloc::api::tryMalloc(unsigned long, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:43:12
        #5 0x7f33c49703c3 in void* bmalloc::IsoTLS::allocateSlow<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:98:20
        #6 0x7f33c4970268 in void* bmalloc::IsoTLS::allocateImpl<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:76:16
        #7 0x7f33c49701b4 in void* bmalloc::IsoTLS::allocate<WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:42:12
        #8 0x7f33c4953f60 in bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>::allocate()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoHeapInlines.h:60:12
        #9 0x7f33c494de52 in WebCore::MediaElementAudioSourceNode::operator new(unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:46:1
        #10 0x7f33c494e22c in WebCore::MediaElementAudioSourceNode::create(WebCore::BaseAudioContext&,
WebCore::MediaElementAudioSourceOptions&&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:60:27
        #11 0x7f33c483417c in WebCore::AudioContext::createMediaElementSource(WebCore::HTMLMediaElement&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/AudioContext.cpp:133:12
        #12 0x7f33ca1af238 in WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSourceBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSAudioContext*) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/WebCore/JSAudioContext.cpp:339:5
        #13 0x7f33ca1a1023 in long WebCore::IDLOperation<WebCore::JSAudioContext>::call<&
(WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSourceBody(JSC::JSGlobalObject*, JSC::CallFrame*, WebCore::JSAudioContext*)),
(WebCore::CastedThisErrorBehavior)0>(JSC::JSGlobalObject&, JSC::CallFrame&, char const*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSDOMOperation.h:53:9
        #14 0x7f33ca1a0b63 in WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSource(JSC::JSGlobalObject*, JSC::CallFrame*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/WebCore/JSAudioContext.cpp:344:12
        #15 0x7f335b13d177  (<unknown module>)
        #16 0x7f33b911a335  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/lib/libjavascriptcoregtk-4.0.so.18+0x790d335)
        #17 0x7f33b90f9d61  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/lib/libjavascriptcoregtk-4.0.so.18+0x78ecd61)
        #18 0x7f33b751a1a4 in JSC::JITCode::execute(JSC::VM*, JSC::ProtoCallFrame*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/jit/JITCodeInlines.h:42:38
        #19 0x7f33b7500e60 in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/interpreter/Interpreter.cpp:904:27
        #20 0x7f33b7dc5f9d in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:57:28
        #21 0x7f33b7dc6461 in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&,
WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:64:22
        #22 0x7f33b7dc6e14 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:85:12
        #23 0x7f33c4e9a977 in WebCore::JSExecState::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData
const&, JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSExecState.h:73:16
        #24 0x7f33c4f78cf9 in WebCore::JSEventListener::handleEvent(WebCore::ScriptExecutionContext&, WebCore::Event&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/bindings/js/JSEventListener.cpp:179:22
        #25 0x7f33c5c32290 in WebCore::EventTarget::innerInvokeEventListeners(WebCore::Event&,
WTF::Vector<WTF::RefPtr<WebCore::RegisteredEventListener, WTF::DumbPtrTraits<WebCore::RegisteredEventListener> >, 1ul, WTF::CrashOnOverflow,
16ul, WTF::FastMalloc>, WebCore::EventTarget::EventInvokePhase) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/EventTarget.cpp:341:40
        #26 0x7f33c5c2a5dc in WebCore::EventTarget::fireEventListeners(WebCore::Event&, WebCore::EventTarget::EventInvokePhase)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/dom/EventTarget.cpp:273:9
        #27 0x7f33c5c31875 in WebCore::EventTarget::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/EventTarget.cpp:222:5
        #28 0x7f33c490d88d in WebCore::BaseAudioContext::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/BaseAudioContext.cpp:1102:18
        #29 0x7f33c5c6af61 in WebCore::MainThreadGenericEventQueue::dispatchOneEvent() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/GenericEventQueue.cpp:75:12
```

Later `eventhandler4` is executed periodicaly where `close` method is called on `audioCtx`:

```
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
```

That cause that all connected/related audio nodes with `audioCtx`(AudioContext) are disconnected and eventually freed. Among them `MediaElementAudioSourceNode`.

```
0x611000352b08 is located 200 bytes inside of 248-byte region [0x611000352a40,0x611000352b38)
freed by thread T0 here:
        #0 0x49495d in free (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x49495d)
        #1 0x7f33b9382f98 in bmalloc::DebugHeap::free(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/bmalloc/bmalloc/DebugHeap.cpp:120:5
        #2 0x7f33b937f603 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/Cache.cpp:85:20
        #3 0x7f33c413e39e in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:105:16
        #4 0x7f33c413e35a in bmalloc::api::free(void*, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:86:5
        #5 0x7f33c4970ed1 in void bmalloc::IsoTLS::deallocateSlow<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:145:20
        #6 0x7f33c4970d30 in void bmalloc::IsoTLS::deallocateImpl<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:122:9
        #7 0x7f33c4970c7c in void bmalloc::IsoTLS::deallocate<WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:50:5
        #8 0x7f33c4953f8c in bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>::deallocate(void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoHeapInlines.h:73:5
        #9 0x7f33c494de7c in WebCore::MediaElementAudioSourceNode::operator delete(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:46:1
        #10 0x7f33c494e9f7 in WebCore::MediaElementAudioSourceNode::~MediaElementAudioSourceNode()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:81:1
        #11 0x7f33c4901050 in WebCore::BaseAudioContext::deleteMarkedNodes() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/BaseAudioContext.cpp:849:13
        #12 0x7f33c4898153 in WebCore::AudioNode::deref(WebCore::AudioNode::RefType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/AudioNode.cpp:488:19
        #13 0x7f33c483cf56 in WebCore::AudioNode::derefEventTarget() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/AudioNode.h:242:40
        #14 0x7f33c148e810 in WebCore::EventTarget::deref() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/WebCore/EventTarget.h:60:20
        #15 0x7f33c2387da5 in WTF::Ref<WebCore::EventTarget, WTF::DumbPtrTraits<WebCore::EventTarget> >::~Ref()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Ref.h:61:39
        #16 0x7f33c239079d in WebCore::JSDOMWrapper<WebCore::EventTarget>::~JSDOMWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSDOMWrapper.h:72:46
        #17 0x7f33c238abd7 in WebCore::JSEventTarget::~JSEventTarget() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/WebCore/JSEventTarget.h:30:7
        #18 0x7f33c235ef0c in WebCore::JSEventTarget::destroy(JSC::JSCell*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/WebCore/JSEventTarget.cpp:262:32
        #19 0x7f33b809c0a3 in JSC::JSDestructibleObjectDestroyFunc::operator()(JSC::VM&, JSC::JSCell*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:38:9
        #20 0x7f33b80798b5 in JSC::JSDestructibleObjectHeapCellType::destroy(JSC::VM&, JSC::JSCell*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:58:5
        #21 0x7f33b71c15af in JSC::Subspace::destroy(JSC::VM&, JSC::JSCell*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Subspace.cpp:65:21
        #22 0x7f33b71c1124 in JSC::PreciseAllocation::sweep() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/PreciseAllocation.cpp:230:25
        #23 0x7f33b7181f8b in JSC::MarkedSpace::sweepPreciseAllocations() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/MarkedSpace.cpp:234:21
        #24 0x7f33b705e5f5 in JSC::Heap::sweepInFinalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2150:19
        #25 0x7f33b705de69 in JSC::Heap::finalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2095:9
        #26 0x7f33b705ccf9 in JSC::Heap::handleNeedFinalize(unsigned int) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2016:9
        #27 0x7f33b705b6f5 in JSC::Heap::handleNeedFinalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2032:12
        #28 0x7f33b70538d1 in JSC::Heap::finishChangingPhase(JSC::GCConductor) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:1603:17
        #29 0x7f33b705755b in JSC::Heap::changePhase(JSC::GCConductor, JSC::CollectorPhase) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:1577:12
```

Because `MediaElementAudioSourceNode` node inherits from `AudioSourceProviderClient`

```
https://github.com/WebKit/webkit/blob/950143da027e80924b4bb86defa8a3f21fd3fb1e/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.h
#L40

class MediaElementAudioSourceNode final : public AudioNode, public AudioSourceProviderClient {
```

it receives some kind of internal notification during standard WebAudio processing. Unfortunatelly before that notification handling happens, there is no check whether references to `MediaElementAudioSourceNode` are still valid which in our scenario leads to a use-after-free vulnerability:

```
Vulnerable line:
https://github.com/WebKit/webkit/blob/950143da027e80924b4bb86defa8a3f21fd3fb1e/Source/WebCore/platform/audio/gstreamer/AudioSourceProviderGS
treamer.cpp#L382
m_client->setFormat(m_deinterleaveSourcePads, gSampleBitRate); //m_client == AudioSourceProviderClient == MediaElementAudioSourceNode

==68844==ERROR: AddressSanitizer: heap-use-after-free on address 0x611000352b08 at pc 0x7f33c9f8f887 bp 0x7ffc651073d0 sp 0x7ffc651073c8
READ of size 8 at 0x611000352b08 thread T0
        #0 0x7f33c9f8f886 in WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/platform/audio/gstreamer/AudioSourceProviderGStreamer.cpp:382:19
        #1 0x7f33c9f8ff5d in WTF::Detail::CallableWrapper<WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0,
void>::call() /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #2 0x7f33befa565e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #3 0x7f33c9f90c78 in void
WebCore::MainThreadNotifier<WebCore::AudioSourceProviderGStreamer::MainThreadNotification>::notify<WebCore::AudioSourceProviderGStreamer::de
interleavePadsConfigured()::$_0>(WebCore::AudioSourceProviderGStreamer::MainThreadNotification,
WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0&&)::'lambda'()::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/platform/graphics/gstreamer/MainThreadNotifier.h:64:17
        #4 0x7f33c9f90b8d in WTF::Detail::CallableWrapper<void
WebCore::MainThreadNotifier<WebCore::AudioSourceProviderGStreamer::MainThreadNotification>::notify<WebCore::AudioSourceProviderGStreamer::de
interleavePadsConfigured()::$_0>(WebCore::AudioSourceProviderGStreamer::MainThreadNotification,
WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0&&)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #5 0x7f33b649df1e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #6 0x7f33b91bd007 in WTF::RunLoop::performWork() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/RunLoop.cpp:119:9
        #7 0x7f33b934e0bb in WTF::RunLoop::RunLoop()::$_1::operator()(void*) const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:80:42
        #8 0x7f33b934e094 in WTF::RunLoop::RunLoop()::$_1::__invoke(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:79:43
        #9 0x7f33b934e022 in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #10 0x7f33b934bd54 in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #11 0x7f33aa18b284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #12 0x7f33aa18b64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #13 0x7f33aa18b961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #14 0x7f33b934c786 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #15 0x7f33c1b7ce8c in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #16 0x7f33c1b7a0da in WebKit::WebProcessMain(int, char**) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebKit/WebProcess/gtk/WebProcessMainGtk.cpp:66:12
        #17 0x4c6c45 in main /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebKit/WebProcess/EntryPoint/unix/WebProcessMain.cpp:45:12
        #18 0x7f33a6370b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #19 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x41ccd9)
```

Proper heap grooming can give an attacker full control of this use-after-free vulnerability and as a result could allow it to be turned into a arbitrary code execution.

Crash Information

```
icewall@ubuntu:~/webkitgtk-2.30.1/code/build/bin$ ./MiniBrowser --autoplay-policy=allow --enable-write-console-messages-to-stdout=true
http://localhost/poc.html
http://localhost/poc.html:50:28: CONSOLE LOG Start fuzzing
http://localhost/poc.html:65:28: CONSOLE LOG OfflineAudioContext::startRendering
http://localhost/poc.html:25:16: CONSOLE LOG eventhandler5
http://localhost/poc.html:26:16: CONSOLE LOG ============
http://localhost/poc.html:27:16: CONSOLE LOG event type :  statechange
http://localhost/poc.html:28:16: CONSOLE LOG OfflineAudioContext.state :  running
http://localhost/poc.html:31:16: CONSOLE LOG    audioElement.load();
http://localhost/poc.html:36:20: CONSOLE LOG    audioCtx.createMediaElementSource( audioElement );
http://localhost/poc.html:41:16: CONSOLE LOG    setInterval(eventhandler4,53);
http://localhost/poc.html:25:16: CONSOLE LOG eventhandler5
http://localhost/poc.html:26:16: CONSOLE LOG ============
http://localhost/poc.html:27:16: CONSOLE LOG event type :  statechange
http://localhost/poc.html:28:16: CONSOLE LOG OfflineAudioContext.state :  closed
http://localhost/poc.html:31:16: CONSOLE LOG    audioElement.load();
http://localhost/poc.html:38:29: CONSOLE LOG InvalidStateError: Media element is already associated with an audio source node
http://localhost/poc.html:41:16: CONSOLE LOG    setInterval(eventhandler4,53);
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
http://localhost/poc.html:11:16: CONSOLE LOG eventhandler4
http://localhost/poc.html:12:16: CONSOLE LOG ==============
http://localhost/poc.html:15:16: CONSOLE LOG    audioCtx.close( );
=================================================================
==68844==ERROR: AddressSanitizer: heap-use-after-free on address 0x611000352b08 at pc 0x7f33c9f8f887 bp 0x7ffc651073d0 sp 0x7ffc651073c8
READ of size 8 at 0x611000352b08 thread T0
        #0 0x7f33c9f8f886 in WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/platform/audio/gstreamer/AudioSourceProviderGStreamer.cpp:382:19
        #1 0x7f33c9f8ff5d in WTF::Detail::CallableWrapper<WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0,
void>::call() /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #2 0x7f33befa565e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #3 0x7f33c9f90c78 in void
WebCore::MainThreadNotifier<WebCore::AudioSourceProviderGStreamer::MainThreadNotification>::notify<WebCore::AudioSourceProviderGStreamer::de
interleavePadsConfigured()::$_0>(WebCore::AudioSourceProviderGStreamer::MainThreadNotification,
WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0&&)::'lambda'()::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/platform/graphics/gstreamer/MainThreadNotifier.h:64:17
        #4 0x7f33c9f90b8d in WTF::Detail::CallableWrapper<void
WebCore::MainThreadNotifier<WebCore::AudioSourceProviderGStreamer::MainThreadNotification>::notify<WebCore::AudioSourceProviderGStreamer::de
interleavePadsConfigured()::$_0>(WebCore::AudioSourceProviderGStreamer::MainThreadNotification,
WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0&&)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #5 0x7f33b649df1e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #6 0x7f33b91bd007 in WTF::RunLoop::performWork() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/RunLoop.cpp:119:9
        #7 0x7f33b934e0bb in WTF::RunLoop::RunLoop()::$_1::operator()(void*) const /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:80:42
        #8 0x7f33b934e094 in WTF::RunLoop::RunLoop()::$_1::__invoke(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:79:43
        #9 0x7f33b934e022 in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #10 0x7f33b934bd54 in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #11 0x7f33aa18b284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #12 0x7f33aa18b64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #13 0x7f33aa18b961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #14 0x7f33b934c786 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #15 0x7f33c1b7ce8c in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #16 0x7f33c1b7a0da in WebKit::WebProcessMain(int, char**) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebKit/WebProcess/gtk/WebProcessMainGtk.cpp:66:12
        #17 0x4c6c45 in main /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebKit/WebProcess/EntryPoint/unix/WebProcessMain.cpp:45:12
        #18 0x7f33a6370b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #19 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x41ccd9)

0x611000352b08 is located 200 bytes inside of 248-byte region [0x611000352a40,0x611000352b38)
freed by thread T0 here:
        #0 0x49495d in free (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x49495d)
        #1 0x7f33b9382f98 in bmalloc::DebugHeap::free(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/bmalloc/bmalloc/DebugHeap.cpp:120:5
        #2 0x7f33b937f603 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/Cache.cpp:85:20
        #3 0x7f33c413e39e in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:105:16
        #4 0x7f33c413e35a in bmalloc::api::free(void*, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:86:5
        #5 0x7f33c4970ed1 in void bmalloc::IsoTLS::deallocateSlow<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:145:20
        #6 0x7f33c4970d30 in void bmalloc::IsoTLS::deallocateImpl<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:122:9
        #7 0x7f33c4970c7c in void bmalloc::IsoTLS::deallocate<WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:50:5
        #8 0x7f33c4953f8c in bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>::deallocate(void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoHeapInlines.h:73:5
        #9 0x7f33c494de7c in WebCore::MediaElementAudioSourceNode::operator delete(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:46:1
        #10 0x7f33c494e9f7 in WebCore::MediaElementAudioSourceNode::~MediaElementAudioSourceNode()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:81:1
        #11 0x7f33c4901050 in WebCore::BaseAudioContext::deleteMarkedNodes() /home/icewall/tools/fuzzing/browsers/webkitgtk-
```

```
2.30.1/code/Source/WebCore/Modules/webaudio/BaseAudioContext.cpp:849:13
        #12 0x7f33c4898153 in WebCore::AudioNode::deref(WebCore::AudioNode::RefType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/AudioNode.cpp:488:19
        #13 0x7f33c483cf56 in WebCore::AudioNode::derefEventTarget() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/AudioNode.h:242:40
        #14 0x7f33c148e810 in WebCore::EventTarget::deref() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/WebCore/EventTarget.h:60:20
        #15 0x7f33c2387da5 in WTF::Ref<WebCore::EventTarget, WTF::DumbPtrTraits<WebCore::EventTarget> >::~Ref()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/wtf/Ref.h:61:39
        #16 0x7f33c239079d in WebCore::JSDOMWrapper<WebCore::EventTarget>::~JSDOMWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSDOMWrapper.h:72:46
        #17 0x7f33c238abd7 in WebCore::JSEventTarget::~JSEventTarget() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/WebCore/JSEventTarget.h:30:7
        #18 0x7f33c235ef0c in WebCore::JSEventTarget::destroy(JSC::JSCell*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/WebCore/JSEventTarget.cpp:262:32
        #19 0x7f33b809c0a3 in JSC::JSDestructibleObjectDestroyFunc::operator()(JSC::VM&, JSC::JSCell*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:38:9
        #20 0x7f33b80798b5 in JSC::JSDestructibleObjectHeapCellType::destroy(JSC::VM&, JSC::JSCell*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:58:5
        #21 0x7f33b71c15af in JSC::Subspace::destroy(JSC::VM&, JSC::JSCell*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Subspace.cpp:65:21
        #22 0x7f33b71c1124 in JSC::PreciseAllocation::sweep() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/PreciseAllocation.cpp:230:25
        #23 0x7f33b7181f8b in JSC::MarkedSpace::sweepPreciseAllocations() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/MarkedSpace.cpp:234:21
        #24 0x7f33b705e5f5 in JSC::Heap::sweepInFinalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2150:19
        #25 0x7f33b705de69 in JSC::Heap::finalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2095:9
        #26 0x7f33b705ccf9 in JSC::Heap::handleNeedFinalize(unsigned int) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2016:9
        #27 0x7f33b705b6f5 in JSC::Heap::handleNeedFinalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:2032:12
        #28 0x7f33b70538d1 in JSC::Heap::finishChangingPhase(JSC::GCConductor) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:1603:17
        #29 0x7f33b705755b in JSC::Heap::changePhase(JSC::GCConductor, JSC::CollectorPhase) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/heap/Heap.cpp:1577:12

previously allocated by thread T0 here:
        #0 0x494bdd in malloc (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x494bdd)
        #1 0x7f33b9382cfb in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/DebugHeap.cpp:98:20
        #2 0x7f33b937f018 in bmalloc::Cache::tryAllocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/bmalloc/bmalloc/Cache.cpp:57:27
        #3 0x7f33c41265be in bmalloc::Cache::tryAllocate(bmalloc::HeapKind, unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:73:16
        #4 0x7f33c412614a in bmalloc::api::tryMalloc(unsigned long, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:43:12
        #5 0x7f33c49703c3 in void* bmalloc::IsoTLS::allocateSlow<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:98:20
        #6 0x7f33c4970268 in void* bmalloc::IsoTLS::allocateImpl<bmalloc::IsoConfig<248u>, WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:76:16
        #7 0x7f33c49701b4 in void* bmalloc::IsoTLS::allocate<WebCore::MediaElementAudioSourceNode>
(bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>&, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoTLSInlines.h:42:12
        #8 0x7f33c4953f60 in bmalloc::api::IsoHeap<WebCore::MediaElementAudioSourceNode>::allocate()
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/ForwardingHeaders/bmalloc/IsoHeapInlines.h:60:12
        #9 0x7f33c494de52 in WebCore::MediaElementAudioSourceNode::operator new(unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:46:1
        #10 0x7f33c494e22c in WebCore::MediaElementAudioSourceNode::create(WebCore::BaseAudioContext&,
WebCore::MediaElementAudioSourceOptions&&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/MediaElementAudioSourceNode.cpp:60:27
        #11 0x7f33c483417c in WebCore::AudioContext::createMediaElementSource(WebCore::HTMLMediaElement&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/Modules/webaudio/AudioContext.cpp:133:12
        #12 0x7f33ca1af238 in WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSourceBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSAudioContext*) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/WebCore/JSAudioContext.cpp:339:5
        #13 0x7f33ca1a1023 in long WebCore::IDLOperation<WebCore::JSAudioContext>::call<&
(WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSourceBody(JSC::JSGlobalObject*, JSC::CallFrame*, WebCore::JSAudioContext*)),
(WebCore::CastedThisErrorBehavior)0>(JSC::JSGlobalObject&, JSC::CallFrame&, char const*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSDOMOperation.h:53:9
        #14 0x7f33ca1a0b63 in WebCore::jsAudioContextPrototypeFunctionCreateMediaElementSource(JSC::JSGlobalObject*, JSC::CallFrame*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/DerivedSources/WebCore/JSAudioContext.cpp:344:12
        #15 0x7f335b13d177  (<unknown module>)
        #16 0x7f33b911a335  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/lib/libjavascriptcoregtk-4.0.so.18+0x790d335)
        #17 0x7f33b90f9d61  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/build/lib/libjavascriptcoregtk-4.0.so.18+0x78ecd61)
        #18 0x7f33b751a1a4 in JSC::JITCode::execute(JSC::VM*, JSC::ProtoCallFrame*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/jit/JITCodeInlines.h:42:38
        #19 0x7f33b7500e60 in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/interpreter/Interpreter.cpp:904:27
        #20 0x7f33b7dc5f9d in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:57:28
        #21 0x7f33b7dc6461 in JSC::call(JSC::JSGlobalObject*, JSC::JSValue, JSC::CallData const&, JSC::JSValue, JSC::ArgList const&,
WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:64:22
        #22 0x7f33b7dc6e14 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/JavaScriptCore/runtime/CallData.cpp:85:12
        #23 0x7f33c4e9a977 in WebCore::JSExecState::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData
const&, JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/bindings/js/JSExecState.h:73:16
        #24 0x7f33c4f78cf9 in WebCore::JSEventListener::handleEvent(WebCore::ScriptExecutionContext&, WebCore::Event&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/bindings/js/JSEventListener.cpp:179:22
        #25 0x7f33c5c32290 in WebCore::EventTarget::innerInvokeEventListeners(WebCore::Event&,
WTF::Vector<WTF::RefPtr<WebCore::RegisteredEventListener, WTF::DumbPtrTraits<WebCore::RegisteredEventListener> >, 1ul, WTF::CrashOnOverflow,
16ul, WTF::FastMalloc>, WebCore::EventTarget::EventInvokePhase) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/EventTarget.cpp:341:40
        #26 0x7f33c5c2a5dc in WebCore::EventTarget::fireEventListeners(WebCore::Event&, WebCore::EventTarget::EventInvokePhase)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.1/code/Source/WebCore/dom/EventTarget.cpp:273:9
        #27 0x7f33c5c31875 in WebCore::EventTarget::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/EventTarget.cpp:222:5
        #28 0x7f33c490d88d in WebCore::BaseAudioContext::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/Modules/webaudio/BaseAudioContext.cpp:1102:18
        #29 0x7f33c5c6af61 in WebCore::MainThreadGenericEventQueue::dispatchOneEvent() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/dom/GenericEventQueue.cpp:75:12

SUMMARY: AddressSanitizer: heap-use-after-free /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.1/code/Source/WebCore/platform/audio/gstreamer/AudioSourceProviderGStreamer.cpp:382:19 in
WebCore::AudioSourceProviderGStreamer::deinterleavePadsConfigured()::$_0::operator()() const
Shadow bytes around the buggy address:
  0x0c2280062510: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x0c2280062520: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2280062530: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2280062540: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c2280062550: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c2280062560: fd[fd]fd fd fd fd fd fa fa fa fa fa fa fa fa fa
  0x0c2280062570: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

```
  0x0c2280062580: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c2280062590: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c22800625a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c22800625b0: fd fd fd fd fd fd fd fd 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
==68844==ABORTING
```

Timeline

2020-10-20 - Vendor Disclosure

2020-02-15 - Vendor Released

2020-03-03 - Public Release

CREDIT

Discovered by Marcin 'Icewall' Noga of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2019-0955

NEXT REPORT TALOS-2020-1221