Talos Vulnerability Report

TALOS-2020-1155

# Webkit WebSocket code execution vulnerability

NOVEMBER 30, 2020

### CVE NUMBER

CVE-2020-13543

### Summary

A code execution vulnerability exists in the WebSocket functionality of Webkit WebKitGTK 2.30.0. A specially crafted web page can trigger a use-after-free vulnerability which can lead to remote code execution. An attacker can get a user to visit a webpage to trigger this vulnerability.

### Tested Versions

Webkit WebKitGTK 2.30.0

### 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 the `WebSocket` variable and the way it is handled during the document reloads. A malicious web page can lead to a use-after-free vulnerability and potential remote code execution.

To understand the vulnerability we will focus on script parts of the `poc.html` file because `index.html` should be straight forward. In function `func_1` a reference to an `index.html` (parent) is obtained in `line 19`.

```
Line 18   parent_doc = window.top.document;
Line 19   html_obj = parent_doc.all[0];
```

Next `eventhandler1` func is executed where `WebSocket` object is created `line 28`. Further, inside/just before WebSocket is closed in `line 30` assigned `onerror` event handler `free_it` is executed.

```
Line 26 function eventhandler1(event)
Line 27 {
(...)
Line 29   try { ws.onerror = free_it; } catch(e) { }
Line 30   try { ws.close(); } catch(e) { }
```

Adding parent html object to current document body `line 35` cause an “interesting” case where among the others WebSocket object `ws` is released.

```
Line 33 function free_it()
Line 34 {
Line 35   try { document.body.appendChild(html_obj); } catch(e) { }
Line 36 }
```

We can observe it on an ASAN output:

```
0x6110002c0cd8 is located 88 bytes inside of 200-byte region [0x6110002c0c80,0x6110002c0d48)
freed by thread T0 here:
        #0 0x49494d in free (/home/icewall/projects/webkit/build/bin/WebKitWebProcess+0x49494d)
        #1 0x7f60c6359bbc in non-virtual thunk to WebCore::WebSocket::stop() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4266bbc)
        #2 0x7f60c720fdb5 in WebCore::ScriptExecutionContext::stopActiveDOMObjects() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x511cdb5)
        #3 0x7f60c816f62b in WebCore::FrameLoader::frameDetached() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x607c62b)
        #4 0x7f60c7737f98 in WebCore::HTMLFrameOwnerElement::disconnectContentFrame()
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x5644f98)
        #5 0x7f60c6ec910f in WebCore::ContainerNode::removeChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4dd610f)
        #6 0x7f60c6ec5036 in WebCore::collectChildrenAndRemoveFromOldParent(WebCore::Node&, WTF::Vector<WTF::Ref<WebCore::Node,
WTF::DumbPtrTraits<WebCore::Node> >, 11ul, WTF::CrashOnOverflow, 16ul, WTF::FastMalloc>&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x4dd2036)
        #7 0x7f60c6ec38b4 in WebCore::ContainerNode::appendChildWithoutPreInsertionValidityCheck(WebCore::Node&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x4dd08b4)
        #8 0x7f60c6ecd459 in WebCore::ContainerNode::appendChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4dda459)
        #9 0x7f60c715b658 in WebCore::Node::appendChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x5068658)
        #10 0x7f606674b177  (<unknown module>)
        #11 0x7f60c0f691e0  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x454f1e0)
        #12 0x7f60c0f4f748  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x4535748)
        #13 0x7f60bf36132a in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x294732a)
        #14 0x7f60bfd77159 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-
4.0.so.18+0x335d159)

previously allocated by thread T0 here:
        #0 0x494bcd in malloc (/home/icewall/projects/webkit/build/bin/WebKitWebProcess+0x494bcd)
        #1 0x7f60c113a08a in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
(/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x472008a)
        #2 0x7f60c633c98c in WebCore::ThreadableWebSocketChannel::create(WebCore::ScriptExecutionContext&, WebCore::WebSocketChannelClient&,
WebCore::SocketProvider&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x424998c)
        #3 0x7f60c6350d8c in WebCore::WebSocket::connect(WTF::String const&, WTF::Vector<WTF::String, 0ul, WTF::CrashOnOverflow, 16ul,
WTF::FastMalloc> const&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x425dd8c)
        #4 0x7f60c63500a0 in WebCore::WebSocket::create(WebCore::ScriptExecutionContext&, WTF::String const&, WTF::Vector<WTF::String, 0ul,
WTF::CrashOnOverflow, 16ul, WTF::FastMalloc> const&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x425d0a0)
        #5 0x7f60c5bc748d in WebCore::constructJSWebSocket1(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3ad448d)
        #6 0x7f60c5bc5f7d in WebCore::JSDOMConstructor<WebCore::JSWebSocket>::construct(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3ad2f7d)
        #7 0x7f60bf80febb in JSC::LLInt::setUpCall(JSC::CallFrame*, JSC::CodeSpecializationKind, JSC::JSValue, JSC::LLIntCallLinkInfo*)
(/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x2df5ebb)
        #8 0x7f60c0f69e81  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x454fe81)
        #9 0x7f60c0f4f748  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x4535748)
        #10 0x7f60bf36132a in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x294732a)
        #11 0x7f60bfd77159 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-
4.0.so.18+0x335d159)
```

And because that happens just before `ws.close` call at `line 30` its further execution leads to a use-after-free condition:

```
==75258==ERROR: AddressSanitizer: heap-use-after-free on address 0x6110002c0cd8 at pc 0x7f60c45f7a8d bp 0x7ffeff4ba450 sp 0x7ffeff4ba448
READ of size 1 at 0x6110002c0cd8 thread T0
        #0 0x7f60c45f7a8c in non-virtual thunk to WebKit::WebSocketChannel::fail(WTF::String const&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x2504a8c)
        #1 0x7f60c635813e in WebCore::WebSocket::close(WTF::Optional<unsigned short>, WTF::String const&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x426513e)
        #2 0x7f60c5bce576 in WebCore::jsWebSocketPrototypeFunctionClose(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3adb576)
        #3 0x7f606674b177  (<unknown module>)
```

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

```
==75258==ERROR: AddressSanitizer: heap-use-after-free on address 0x6110002c0cd8 at pc 0x7f60c45f7a8d bp 0x7ffeff4ba450 sp 0x7ffeff4ba448
READ of size 1 at 0x6110002c0cd8 thread T0
        #0 0x7f60c45f7a8c in non-virtual thunk to WebKit::WebSocketChannel::fail(WTF::String const&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x2504a8c)
        #1 0x7f60c635813e in WebCore::WebSocket::close(WTF::Optional<unsigned short>, WTF::String const&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x426513e)
        #2 0x7f60c5bce576 in WebCore::jsWebSocketPrototypeFunctionClose(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3adb576)
        #3 0x7f606674b177  (<unknown module>)

0x6110002c0cd8 is located 88 bytes inside of 200-byte region [0x6110002c0c80,0x6110002c0d48)
freed by thread T0 here:
        #0 0x49494d in free (/home/icewall/projects/webkit/build/bin/WebKitWebProcess+0x49494d)
        #1 0x7f60c6359bbc in non-virtual thunk to WebCore::WebSocket::stop() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4266bbc)
        #2 0x7f60c720fdb5 in WebCore::ScriptExecutionContext::stopActiveDOMObjects() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x511cdb5)
        #3 0x7f60c816f62b in WebCore::FrameLoader::frameDetached() (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x607c62b)
        #4 0x7f60c7737f98 in WebCore::HTMLFrameOwnerElement::disconnectContentFrame()
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x5644f98)
        #5 0x7f60c6ec910f in WebCore::ContainerNode::removeChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4dd610f)
        #6 0x7f60c6ec5036 in WebCore::collectChildrenAndRemoveFromOldParent(WebCore::Node&, WTF::Vector<WTF::Ref<WebCore::Node,
WTF::DumbPtrTraits<WebCore::Node> >, 11ul, WTF::CrashOnOverflow, 16ul, WTF::FastMalloc>&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x4dd2036)
        #7 0x7f60c6ec38b4 in WebCore::ContainerNode::appendChildWithoutPreInsertionValidityCheck(WebCore::Node&)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x4dd08b4)
        #8 0x7f60c6ecd459 in WebCore::ContainerNode::appendChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x4dda459)
        #9 0x7f60c715b658 in WebCore::Node::appendChild(WebCore::Node&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-
4.0.so.37+0x5068658)
        #10 0x7f606674b177  (<unknown module>)
        #11 0x7f60c0f691e0  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x454f1e0)
        #12 0x7f60c0f4f748  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x4535748)
        #13 0x7f60bf36132a in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x294732a)
        #14 0x7f60bfd77159 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-
4.0.so.18+0x335d159)

previously allocated by thread T0 here:
        #0 0x494bcd in malloc (/home/icewall/projects/webkit/build/bin/WebKitWebProcess+0x494bcd)
        #1 0x7f60c113a08a in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
(/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x472008a)
        #2 0x7f60c633c98c in WebCore::ThreadableWebSocketChannel::create(WebCore::ScriptExecutionContext&, WebCore::WebSocketChannelClient&,
WebCore::SocketProvider&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x424998c)
        #3 0x7f60c6350d8c in WebCore::WebSocket::connect(WTF::String const&, WTF::Vector<WTF::String, 0ul, WTF::CrashOnOverflow, 16ul,
WTF::FastMalloc> const&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x425dd8c)
        #4 0x7f60c63500a0 in WebCore::WebSocket::create(WebCore::ScriptExecutionContext&, WTF::String const&, WTF::Vector<WTF::String, 0ul,
WTF::CrashOnOverflow, 16ul, WTF::FastMalloc> const&) (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x425d0a0)
        #5 0x7f60c5bc748d in WebCore::constructJSWebSocket1(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3ad448d)
        #6 0x7f60c5bc5f7d in WebCore::JSDOMConstructor<WebCore::JSWebSocket>::construct(JSC::JSGlobalObject*, JSC::CallFrame*)
(/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x3ad2f7d)
        #7 0x7f60bf80febb in JSC::LLInt::setUpCall(JSC::CallFrame*, JSC::CodeSpecializationKind, JSC::JSValue, JSC::LLIntCallLinkInfo*)
(/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x2df5ebb)
        #8 0x7f60c0f69e81  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x454fe81)
        #9 0x7f60c0f4f748  (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x4535748)
        #10 0x7f60bf36132a in JSC::Interpreter::executeCall(JSC::JSGlobalObject*, JSC::JSObject*, JSC::CallData const&, JSC::JSValue,
JSC::ArgList const&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-4.0.so.18+0x294732a)
        #11 0x7f60bfd77159 in JSC::profiledCall(JSC::JSGlobalObject*, JSC::ProfilingReason, JSC::JSValue, JSC::CallData const&,
JSC::JSValue, JSC::ArgList const&, WTF::NakedPtr<JSC::Exception>&) (/home/icewall/projects/webkit/build/lib/libjavascriptcoregtk-
4.0.so.18+0x335d159)

SUMMARY: AddressSanitizer: heap-use-after-free (/home/icewall/projects/webkit/build/lib/libwebkit2gtk-4.0.so.37+0x2504a8c) in non-virtual
thunk to WebKit::WebSocketChannel::fail(WTF::String const&)
Shadow bytes around the buggy address:
  0x0c2280050140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2280050150: 00 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
  0x0c2280050160: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c2280050170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c2280050180: 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c2280050190: fd fd fd fd fd fd fd fd fd fd[fd]fd fd fd fd fd
  0x0c22800501a0: fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa
  0x0c22800501b0: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c22800501c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c22800501d0: 00 00 00 00 00 00 00 00 fa fa fa fa fa fa fa fa
  0x0c22800501e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
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
==75258==ABORTING
AddressSanitizer:DEADLYSIGNAL
=================================================================
```

Exploit Proof of Concept

1. Unpack WebKit_WebSocket_POC.zip to a directory of your local web server.
2. Build webkit with –asan –release flags
3. Using Minibrowser navigate to an address pointing on an attached index_new.html

4. Observe asan log in the console.

### Credit

Discovered by Marcin ‘Icewall' Noga of Cisco Talos.

https://talosintelligence.com/vulnerability_reports/

### Timeline

2020-09-21 - Vendor Disclosure
2020-11-19 - Vendor Patched
2020-11-30 - Public Release

### CREDIT

Discovered by Marcin 'Icewall' Noga of Cisco Talos.

---

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1126

NEXT REPORT TALOS-2020-1195