Talos Vulnerability Report

TALOS-2020-1195

Webkit ImageDecoderGStreamer use-after-free vulnerability

NOVEMBER 30, 2020

CVE NUMBER

CVE-2020-13584

Summary

An exploitable use-after-free vulnerability exists in WebKitGTK browser version 2.30.1 x64. A specially crafted HTML web page can cause a use-after-free condition, resulting in a remote code execution. The victim needs to visit a malicious web site to trigger this vulnerability.

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 the `ImageDecoderGStreamer` interface, being more precise, the way its handled during `<image>` tag initialization. A malicious web page can trigger a use-after-free vulnerability which could result in remote code execution.

Triggering the vulnerability is relativly simple. An attacker just needs to create a malicious page where the `image` tag is set to one of the following: - the mimetype of data URL is set to one of mimetypes supported by `GStreamer` decoder - the url points to a resource with a content type supported by `GStreamer` decoder

First we see an allocation of `ImageDecoderGStreamer`:

```
previously allocated by thread T0 here:
        #0 0x494bdd in malloc (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x494bdd)
        #1 0x7f8ba51c3cfb in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/DebugHeap.cpp:98:20
        #2 0x7f8ba51c0195 in bmalloc::Cache::allocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/Cache.cpp:64:27
        #3 0x7f8ba4fa0dee in bmalloc::Cache::allocate(bmalloc::HeapKind, unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:81:16
        #4 0x7f8ba4fa0baa in bmalloc::api::malloc(unsigned long, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:49:12
        #5 0x7f8ba4f9fcca in WTF::fastMalloc(unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/FastMalloc.cpp:477:20
        #6 0x7f8bb5d03e84 in WebCore::ImageDecoderGStreamer::operator new(unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:39:5
        #7 0x7f8bb5cfa39c in WebCore::ImageDecoderGStreamer::create(WebCore::SharedBuffer&, WTF::String const&, WebCore::AlphaOption,
WebCore::GammaAndColorProfileOption) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.cpp:85:22
        #8 0x7f8bb3acfc38 in WebCore::ImageDecoder::create(WebCore::SharedBuffer&, WTF::String const&, WebCore::AlphaOption,
WebCore::GammaAndColorProfileOption) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageDecoder.cpp:58:16
        #9 0x7f8bb3ad2386 in WebCore::ImageSource::ensureDecoderAvailable(WebCore::SharedBuffer*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/ImageSource.cpp:78:17
        #10 0x7f8bb3ad2d05 in WebCore::ImageSource::setData(WebCore::SharedBuffer*, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageSource.cpp:99:19
        #11 0x7f8bb3ad2f32 in WebCore::ImageSource::dataChanged(WebCore::SharedBuffer*, bool)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/ImageSource.cpp:113:5
        #12 0x7f8bb38b6766 in WebCore::BitmapImage::dataChanged(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/BitmapImage.cpp:117:22
        #13 0x7f8bb3ac335d in WebCore::Image::setData(WTF::RefPtr<WebCore::SharedBuffer, WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&,
bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/Image.cpp:111:12
        #14 0x7f8bb2f6b2f2 in WebCore::CachedImage::updateImageData(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:549:41
        #15 0x7f8bb2f6ad25 in WebCore::CachedImage::updateBufferInternal(WebCore::SharedBuffer&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/cache/CachedImage.cpp:495:29
        #16 0x7f8bb2f6b768 in WebCore::CachedImage::updateBuffer(WebCore::SharedBuffer&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:557:5
        #17 0x7f8bb2eab594 in WebCore::SubresourceLoader::didReceiveDataOrBuffer(char const*, int, WTF::RefPtr<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:537:25
        #18 0x7f8bb2eab88e in WebCore::SubresourceLoader::didReceiveBuffer(WTF::Ref<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:517:5
        #19 0x7f8bb2e84bf9 in auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()<WTF::Optional<WebCore::DataURLDecoder::Result> >
(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'()::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/ResourceLoader.cpp:284:23
        #20 0x7f8bb2e8495d in WTF::Detail::CallableWrapper<auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()
<WTF::Optional<WebCore::DataURLDecoder::Result> >(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #21 0x7f8baade665e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #22 0x7f8baaed5306 in WTF::CompletionHandler<void ()>::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:62:16
        #23 0x7f8babdb5c91 in WTF::CompletionHandlerCallingScope::~CompletionHandlerCallingScope()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:145:13
        #24 0x7f8bb2eaaa05 in WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&, WTF::CompletionHandler<void
()>&&)::$_7::~$_7() /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/SubresourceLoader.cpp:451:50
        #25 0x7f8bb2ed731d in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #26 0x7f8bb2ed734b in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #27 0x7f8baadecfcf in std::default_delete<WTF::Detail::CallableWrapperBase<void> >::operator()
(WTF::Detail::CallableWrapperBase<void>*) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:78:2
        #28 0x7f8baadeced4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void>,
std::default_delete<WTF::Detail::CallableWrapperBase<void> > >::~unique_ptr() /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:263:4
        #29 0x7f8baade5234 in WTF::Function<void ()>::~Function() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:59:26
```

Later on, when `CacheImage` component detects an invalid image format `ImageDecoderGStreamer` is de-allocated:

```
0x610000028450 is located 16 bytes inside of 192-byte region [0x610000028440,0x610000028500)
freed by thread T0 here:
        #0 0x49495d in free (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x49495d)
        #1 0x7f8ba51c3f98 in bmalloc::DebugHeap::free(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/bmalloc/bmalloc/DebugHeap.cpp:120:5
        #2 0x7f8ba51c0603 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/Cache.cpp:85:20
        #3 0x7f8ba4fa16ee in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:105:16
        #4 0x7f8ba4fa0c0a in bmalloc::api::free(void*, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:86:5
        #5 0x7f8ba4fa0306 in WTF::fastFree(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/FastMalloc.cpp:509:5
        #6 0x7f8bb5d08a14 in WebCore::ImageDecoderGStreamer::operator delete(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:39:5
        #7 0x7f8bb5d052c7 in WebCore::ImageDecoderGStreamer::~ImageDecoderGStreamer() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:44:46
        #8 0x7f8bb3afb59a in WTF::ThreadSafeRefCounted<WebCore::ImageDecoder, (WTF::DestructionThread)0>::deref()
const::'lambda'()::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/ThreadSafeRefCounted.h:117:13
        #9 0x7f8bb3afb493 in WTF::ThreadSafeRefCounted<WebCore::ImageDecoder, (WTF::DestructionThread)0>::deref() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/ThreadSafeRefCounted.h:135:9
        #10 0x7f8bb3afd686 in void WTF::derefIfNotNull<WebCore::ImageDecoder>(WebCore::ImageDecoder*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/RefPtr.h:44:14
        #11 0x7f8bb3ae92f9 in WTF::RefPtr<WebCore::ImageDecoder, WTF::DumbPtrTraits<WebCore::ImageDecoder> >::operator=(std::nullptr_t)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/RefPtr.h:156:5
        #12 0x7f8bb3ad2df0 in WebCore::ImageSource::resetData(WebCore::SharedBuffer*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageSource.cpp:107:15
        #13 0x7f8bb38b6453 in WebCore::BitmapImage::destroyDecodedData(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/BitmapImage.cpp:93:19
        #14 0x7f8bb2f688a3 in WebCore::CachedImage::destroyDecodedData() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:622:18
        #15 0x7f8bb2f6866b in WebCore::CachedImage::clear() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:365:5
        #16 0x7f8bb2f6b3a8 in WebCore::CachedImage::error(WebCore::CachedResource::Status) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:603:5
        #17 0x7f8bb2f6adbf in WebCore::CachedImage::updateBufferInternal(WebCore::SharedBuffer&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/cache/CachedImage.cpp:503:9
        #18 0x7f8bb2f6b768 in WebCore::CachedImage::updateBuffer(WebCore::SharedBuffer&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:557:5
        #19 0x7f8bb2eab594 in WebCore::SubresourceLoader::didReceiveDataOrBuffer(char const*, int, WTF::RefPtr<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:537:25
        #20 0x7f8bb2eab88e in WebCore::SubresourceLoader::didReceiveBuffer(WTF::Ref<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:517:5
        #21 0x7f8bb2e84bf9 in auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()<WTF::Optional<WebCore::DataURLDecoder::Result> >
(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'()::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/ResourceLoader.cpp:284:23
        #22 0x7f8bb2e8495d in WTF::Detail::CallableWrapper<auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()
<WTF::Optional<WebCore::DataURLDecoder::Result> >(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #23 0x7f8baade665e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #24 0x7f8baaed5306 in WTF::CompletionHandler<void ()>::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:62:16
        #25 0x7f8babdb5c91 in WTF::CompletionHandlerCallingScope::~CompletionHandlerCallingScope()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:145:13
        #26 0x7f8bb2eaaa05 in WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&, WTF::CompletionHandler<void
()>&&)::$_7::~$_7() /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/SubresourceLoader.cpp:451:50
        #27 0x7f8bb2ed731d in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #28 0x7f8bb2ed734b in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #29 0x7f8baadecfcf in std::default_delete<WTF::Detail::CallableWrapperBase<void> >::operator()
(WTF::Detail::CallableWrapperBase<void>*) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:78:2
```

Because the reference to the `ImageDecoderGStreamer` is not cleared and checked before later use in `ImageDecoder` it leads to a use-after-free vulnerability:

```
==46942==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000028450 at pc 0x7f8bb5d09026 bp 0x7ffc3e7343c0 sp 0x7ffc3e7343b8
READ of size 8 at 0x610000028450 thread T0
        #0 0x7f8bb5d09025 in std::__uniq_ptr_impl<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::_M_ptr() const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:147:42
        #1 0x7f8bb5d08fe4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::get() const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:332:21
        #2 0x7f8bb5d0a9d4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::operator bool() const
/usr/bin/../lib/gcc/x86_64-linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:346:16
        #3 0x7f8bb5d0a704 in WTF::Function<void (WebCore::EncodedDataStatus)>::operator bool() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:86:47
        #4 0x7f8bb5d0364d in WebCore::ImageDecoderGStreamer::pushEncodedData(WebCore::SharedBuffer const&)::$_6::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.cpp:398:13
        #5 0x7f8bb5d035ed in WTF::Detail::CallableWrapper<WebCore::ImageDecoderGStreamer::pushEncodedData(WebCore::SharedBuffer
const&)::$_6, void>::call() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #6 0x7f8ba22def1e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #7 0x7f8ba4ffe007 in WTF::RunLoop::performWork() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/RunLoop.cpp:119:9
        #8 0x7f8ba518f0bb in WTF::RunLoop::RunLoop()::$_1::operator()(void*) const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:80:42
        #9 0x7f8ba518f094 in WTF::RunLoop::RunLoop()::$_1::__invoke(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:79:43
        #10 0x7f8ba518f022 in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #11 0x7f8ba518cd54 in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #12 0x7f8b95fcc284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #13 0x7f8b95fcc64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #14 0x7f8b95fcc961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #15 0x7f8ba518d786 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #16 0x7f8bad9bde8c in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #17 0x7f8bad9bb0da in WebKit::WebProcessMain(int, char**) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebKit/WebProcess/gtk/WebProcessMainGtk.cpp:66:12
        #18 0x4c6c45 in main /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebKit/WebProcess/EntryPoint/unix/WebProcessMain.cpp:45:12
        #19 0x7f8b921b1b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #20 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/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 arbitrary code execution.

Crash Information

```
icewall@ubuntu:~/tools/fuzzing/browsers/webkitgtk-test/code/build/bin$ ./MiniBrowser http://localhost/webaudio_fuzzer/3.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.

** (WebKitWebProcess:46942): WARNING **: 08:34:26.224: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-0/GstDecodeBin:decodebin0/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.225: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-0/GstDecodeBin:decodebin0/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)

** (WebKitWebProcess:46942): WARNING **: 08:34:26.228: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-1/GstDecodeBin:decodebin1/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.228: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-1/GstDecodeBin:decodebin1/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)

** (WebKitWebProcess:46942): WARNING **: 08:34:26.231: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-2/GstDecodeBin:decodebin2/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.231: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-2/GstDecodeBin:decodebin2/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)

** (WebKitWebProcess:46942): WARNING **: 08:34:26.234: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-3/GstDecodeBin:decodebin3/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.234: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-3/GstDecodeBin:decodebin3/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)

** (WebKitWebProcess:46942): WARNING **: 08:34:26.237: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-4/GstDecodeBin:decodebin4/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.238: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-4/GstDecodeBin:decodebin4/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)

** (WebKitWebProcess:46942): WARNING **: 08:34:26.240: Error: 4, Could not determine type of stream.. Debug output:
gsttypefindelement.c(1168): gst_type_find_element_loop (): /GstPipeline:image-decoder-5/GstDecodeBin:decodebin5/GstTypeFindElement:typefind

** (WebKitWebProcess:46942): WARNING **: 08:34:26.240: Error: 1, Internal data stream error.. Debug output: gsttypefindelement.c(1236):
gst_type_find_element_loop (): /GstPipeline:image-decoder-5/GstDecodeBin:decodebin5/GstTypeFindElement:typefind:
streaming stopped, reason error (-5)
=================================================================
==46942==ERROR: AddressSanitizer: heap-use-after-free on address 0x610000028450 at pc 0x7f8bb5d09026 bp 0x7ffc3e7343c0 sp 0x7ffc3e7343b8
READ of size 8 at 0x610000028450 thread T0
        #0 0x7f8bb5d09025 in std::__uniq_ptr_impl<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::_M_ptr() const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:147:42
        #1 0x7f8bb5d08fe4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::get() const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:332:21
        #2 0x7f8bb5d0a9d4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus>,
std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::operator bool() const
/usr/bin/../lib/gcc/x86_64-linux-gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:346:16
        #3 0x7f8bb5d0a704 in WTF::Function<void (WebCore::EncodedDataStatus)>::operator bool() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:86:47
        #4 0x7f8bb5d0364d in WebCore::ImageDecoderGStreamer::pushEncodedData(WebCore::SharedBuffer const&)::$_6::operator()() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.cpp:398:13
        #5 0x7f8bb5d035ed in WTF::Detail::CallableWrapper<WebCore::ImageDecoderGStreamer::pushEncodedData(WebCore::SharedBuffer
const&)::$_6, void>::call() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #6 0x7f8ba22def1e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #7 0x7f8ba4ffe007 in WTF::RunLoop::performWork() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/RunLoop.cpp:119:9
        #8 0x7f8ba518f0bb in WTF::RunLoop::RunLoop()::$_1::operator()(void*) const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:80:42
        #9 0x7f8ba518f094 in WTF::RunLoop::RunLoop()::$_1::__invoke(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:79:43
        #10 0x7f8ba518f022 in WTF::RunLoop::$_0::operator()(_GSource*, int (*)(void*), void*) const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28
        #11 0x7f8ba518cd54 in WTF::RunLoop::$_0::__invoke(_GSource*, int (*)(void*), void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5
        #12 0x7f8b95fcc284 in g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c284)
        #13 0x7f8b95fcc64f  (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c64f)
        #14 0x7f8b95fcc961 in g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4c961)
        #15 0x7f8ba518d786 in WTF::RunLoop::run() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9
        #16 0x7f8bad9bde8c in int WebKit::AuxiliaryProcessMain<WebKit::WebProcess, WebKit::WebProcessMainGtk>(int, char**)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebKit/Shared/AuxiliaryProcessMain.h:68:5
        #17 0x7f8bad9bb0da in WebKit::WebProcessMain(int, char**) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebKit/WebProcess/gtk/WebProcessMainGtk.cpp:66:12
        #18 0x4c6c45 in main /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebKit/WebProcess/EntryPoint/unix/WebProcessMain.cpp:45:12
        #19 0x7f8b921b1b96 in __libc_start_main /build/glibc-2ORdQG/glibc-2.27/csu/../csu/libc-start.c:310
        #20 0x41ccd9 in _start (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x41ccd9)

0x610000028450 is located 16 bytes inside of 192-byte region [0x610000028440,0x610000028500)
freed by thread T0 here:
        #0 0x49495d in free (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x49495d)
        #1 0x7f8ba51c3f98 in bmalloc::DebugHeap::free(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/bmalloc/bmalloc/DebugHeap.cpp:120:5
        #2 0x7f8ba51c0603 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/Cache.cpp:85:20
        #3 0x7f8ba4fa16ee in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:105:16
        #4 0x7f8ba4fa0c0a in bmalloc::api::free(void*, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:86:5
        #5 0x7f8ba4fa0306 in WTF::fastFree(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/FastMalloc.cpp:509:5
        #6 0x7f8bb5d08a14 in WebCore::ImageDecoderGStreamer::operator delete(void*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:39:5
        #7 0x7f8bb5d052c7 in WebCore::ImageDecoderGStreamer::~ImageDecoderGStreamer() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:44:46
        #8 0x7f8bb3afb59a in WTF::ThreadSafeRefCounted<WebCore::ImageDecoder, (WTF::DestructionThread)0>::deref()
const::'lambda'()::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/ThreadSafeRefCounted.h:117:13
```

```
        #9 0x7f8bb3afb493 in WTF::ThreadSafeRefCounted<WebCore::ImageDecoder, (WTF::DestructionThread)0>::deref() const
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/ThreadSafeRefCounted.h:135:9
        #10 0x7f8bb3afd686 in void WTF::derefIfNotNull<WebCore::ImageDecoder>(WebCore::ImageDecoder*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/RefPtr.h:44:14
        #11 0x7f8bb3ae92f9 in WTF::RefPtr<WebCore::ImageDecoder, WTF::DumbPtrTraits<WebCore::ImageDecoder> >::operator=(std::nullptr_t)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/RefPtr.h:156:5
        #12 0x7f8bb3ad2df0 in WebCore::ImageSource::resetData(WebCore::SharedBuffer*) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageSource.cpp:107:15
        #13 0x7f8bb38b6453 in WebCore::BitmapImage::destroyDecodedData(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/BitmapImage.cpp:93:19
        #14 0x7f8bb2f688a3 in WebCore::CachedImage::destroyDecodedData() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:622:18
        #15 0x7f8bb2f6866b in WebCore::CachedImage::clear() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:365:5
        #16 0x7f8bb2f6b3a8 in WebCore::CachedImage::error(WebCore::CachedResource::Status) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:603:5
        #17 0x7f8bb2f6adbf in WebCore::CachedImage::updateBufferInternal(WebCore::SharedBuffer&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/cache/CachedImage.cpp:503:9
        #18 0x7f8bb2f6b768 in WebCore::CachedImage::updateBuffer(WebCore::SharedBuffer&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:557:5
        #19 0x7f8bb2eab594 in WebCore::SubresourceLoader::didReceiveDataOrBuffer(char const*, int, WTF::RefPtr<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:537:25
        #20 0x7f8bb2eab88e in WebCore::SubresourceLoader::didReceiveBuffer(WTF::Ref<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:517:5
        #21 0x7f8bb2e84bf9 in auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()<WTF::Optional<WebCore::DataURLDecoder::Result> >
(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'()::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/ResourceLoader.cpp:284:23
        #22 0x7f8bb2e8495d in WTF::Detail::CallableWrapper<auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()
<WTF::Optional<WebCore::DataURLDecoder::Result> >(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #23 0x7f8baade665e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #24 0x7f8baaed5306 in WTF::CompletionHandler<void ()>::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:62:16
        #25 0x7f8babdb5c91 in WTF::CompletionHandlerCallingScope::~CompletionHandlerCallingScope()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:145:13
        #26 0x7f8bb2eaaa05 in WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&, WTF::CompletionHandler<void
()>&&)::$_7::~$_7() /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/SubresourceLoader.cpp:451:50
        #27 0x7f8bb2ed731d in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #28 0x7f8bb2ed734b in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #29 0x7f8baadecfcf in std::default_delete<WTF::Detail::CallableWrapperBase<void> >::operator()
(WTF::Detail::CallableWrapperBase<void>*) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:78:2

previously allocated by thread T0 here:
        #0 0x494bdd in malloc (/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/libexec/webkit2gtk-
4.0/WebKitWebProcess+0x494bdd)
        #1 0x7f8ba51c3cfb in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/DebugHeap.cpp:98:20
        #2 0x7f8ba51c0195 in bmalloc::Cache::allocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/bmalloc/bmalloc/Cache.cpp:64:27
        #3 0x7f8ba4fa0dee in bmalloc::Cache::allocate(bmalloc::HeapKind, unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/Cache.h:81:16
        #4 0x7f8ba4fa0baa in bmalloc::api::malloc(unsigned long, bmalloc::HeapKind) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/bmalloc/bmalloc.h:49:12
        #5 0x7f8ba4f9fcca in WTF::fastMalloc(unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WTF/wtf/FastMalloc.cpp:477:20
        #6 0x7f8bb5d03e84 in WebCore::ImageDecoderGStreamer::operator new(unsigned long) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.h:39:5
        #7 0x7f8bb5cfa39c in WebCore::ImageDecoderGStreamer::create(WebCore::SharedBuffer&, WTF::String const&, WebCore::AlphaOption,
WebCore::GammaAndColorProfileOption) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/gstreamer/ImageDecoderGStreamer.cpp:85:22
        #8 0x7f8bb3acfc38 in WebCore::ImageDecoder::create(WebCore::SharedBuffer&, WTF::String const&, WebCore::AlphaOption,
WebCore::GammaAndColorProfileOption) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageDecoder.cpp:58:16
        #9 0x7f8bb3ad2386 in WebCore::ImageSource::ensureDecoderAvailable(WebCore::SharedBuffer*)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/ImageSource.cpp:78:17
        #10 0x7f8bb3ad2d05 in WebCore::ImageSource::setData(WebCore::SharedBuffer*, bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/ImageSource.cpp:99:19
        #11 0x7f8bb3ad2f32 in WebCore::ImageSource::dataChanged(WebCore::SharedBuffer*, bool)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/ImageSource.cpp:113:5
        #12 0x7f8bb38b6766 in WebCore::BitmapImage::dataChanged(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/platform/graphics/BitmapImage.cpp:117:22
        #13 0x7f8bb3ac335d in WebCore::Image::setData(WTF::RefPtr<WebCore::SharedBuffer, WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&,
bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/platform/graphics/Image.cpp:111:12
        #14 0x7f8bb2f6b2f2 in WebCore::CachedImage::updateImageData(bool) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:549:41
        #15 0x7f8bb2f6ad25 in WebCore::CachedImage::updateBufferInternal(WebCore::SharedBuffer&)
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/cache/CachedImage.cpp:495:29
        #16 0x7f8bb2f6b768 in WebCore::CachedImage::updateBuffer(WebCore::SharedBuffer&) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/cache/CachedImage.cpp:557:5
        #17 0x7f8bb2eab594 in WebCore::SubresourceLoader::didReceiveDataOrBuffer(char const*, int, WTF::RefPtr<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:537:25
        #18 0x7f8bb2eab88e in WebCore::SubresourceLoader::didReceiveBuffer(WTF::Ref<WebCore::SharedBuffer,
WTF::DumbPtrTraits<WebCore::SharedBuffer> >&&, long long, WebCore::DataPayloadType) /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/SubresourceLoader.cpp:517:5
        #19 0x7f8bb2e84bf9 in auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()<WTF::Optional<WebCore::DataURLDecoder::Result> >
(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'()::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/Source/WebCore/loader/ResourceLoader.cpp:284:23
        #20 0x7f8bb2e8495d in WTF::Detail::CallableWrapper<auto WebCore::ResourceLoader::loadDataURL()::$_2::operator()
<WTF::Optional<WebCore::DataURLDecoder::Result> >(WTF::Optional<WebCore::DataURLDecoder::Result>)::'lambda'(), void>::call()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:52:39
        #21 0x7f8baade665e in WTF::Function<void ()>::operator()() const /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:83:35
        #22 0x7f8baaed5306 in WTF::CompletionHandler<void ()>::operator()() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:62:16
        #23 0x7f8babdb5c91 in WTF::CompletionHandlerCallingScope::~CompletionHandlerCallingScope()
/home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/build/DerivedSources/ForwardingHeaders/wtf/CompletionHandler.h:145:13
        #24 0x7f8bb2eaaa05 in WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&, WTF::CompletionHandler<void
()>&&)::$_7::~$_7() /home/icewall/tools/fuzzing/browsers/webkitgtk-test/code/Source/WebCore/loader/SubresourceLoader.cpp:451:50
        #25 0x7f8bb2ed731d in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #26 0x7f8bb2ed734b in WTF::Detail::CallableWrapper<WebCore::SubresourceLoader::didReceiveResponse(WebCore::ResourceResponse const&,
WTF::CompletionHandler<void ()>&&)::$_7, void>::~CallableWrapper() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:46:7
        #27 0x7f8baadecfcf in std::default_delete<WTF::Detail::CallableWrapperBase<void> >::operator()
(WTF::Detail::CallableWrapperBase<void>*) const /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:78:2
        #28 0x7f8baadeced4 in std::unique_ptr<WTF::Detail::CallableWrapperBase<void>,
std::default_delete<WTF::Detail::CallableWrapperBase<void> > >::~unique_ptr() /usr/bin/../lib/gcc/x86_64-linux-
```

```
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:263:4
        #29 0x7f8baade5234 in WTF::Function<void ()>::~Function() /home/icewall/tools/fuzzing/browsers/webkitgtk-
test/code/build/DerivedSources/ForwardingHeaders/wtf/Function.h:59:26

SUMMARY: AddressSanitizer: heap-use-after-free /usr/bin/../lib/gcc/x86_64-linux-
gnu/7.5.0/../../../../include/c++/7.5.0/bits/unique_ptr.h:147:42 in std::__uniq_ptr_impl<WTF::Detail::CallableWrapperBase<void,
WebCore::EncodedDataStatus>, std::default_delete<WTF::Detail::CallableWrapperBase<void, WebCore::EncodedDataStatus> > >::_M_ptr() const
Shadow bytes around the buggy address:
  0x0c207fffd030: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x0c207fffd040: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fffd050: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fffd060: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fffd070: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c207fffd080: fa fa fa fa fa fa fa fa fd fd[fd]fd fd fd fd fd
  0x0c207fffd090: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fffd0a0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fffd0b0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c207fffd0c0: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x0c207fffd0d0: 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
==46942==ABORTING

================================================================
```

Timeline

2020-11-02 - Vendor Disclosure

2020-11-23 - Vendor released patch

2020-11-30 - Public Release

CREDIT

Discovered by Marcin 'Icewall' Noga of Cisco Talos.