Talos Vulnerability Report

TALOS-2021-1229

Webkit ImageLoader dispatchPendingErrorEvent use-after-free vulnerability

JUNE 2, 2021

CVE NUMBER

CVE-2021-21775

Summary

A use-after-free vulnerability exists in the way certain events are processed for ImageLoader objects of Webkit WebKitGTK 2.30.4. A specially crafted web page can lead to a potential information leak and further memory corruption. In order to trigger the vulnerability, a victim must be tricked into visiting a malicious webpage.

Tested Versions

Webkit WebKitGTK 2.30.4

Product URLs

https://webkit.org/

CVSSv3 Score

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

CWE

CWE-416 - Use After Free

Details

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

This vulnerabiliy is related to `dispatchPendingErrorEvent` and the way it handles `Image` objects. This even can be triggered when trying to load image an image from non-existant path.

A malicious web page can lead to a use-after-free vulnerability and potential remote code execution.

To understand the steps required to trigger this vulnerability we'll step through parts of the poc.html file and how it manages the allocation of "HTMLImageElement" through dynamic object creation rather than createElement. There are multiple ways to create HTMLImageElement, and 2 of them are used in this proof of concept: 1. Through Javascript: `var img2 = new Image();` 2. Through HTML: `<image> </image>`

When displaying the attached PoC page, the following sequence of events is executed: 1. An associated eventhandler is executed because of an error in static HTMLImageElement `html_image` 2. Event handler code is executed till `adoptNode` which will result in exception, which in turn triggers eventhandler again 3. Same thing happens for the 3rd time (until eventhandler counter is exhausted) when nested event handlres begin to unwind. 4. Rest of the eventhandler is executed 5. Event hander unwinding ends up executing `new ImageData(1024, 1024);` three times. 6. Finally, `onload` handler is triggered which executes `main` function in which `new ImageData(1024, 1024);` and `new Image();` are created. 7. This leads to use-after-free and a crash.

A use after free condition arises when Webkit engine tries to access a stale reference to an object that has already been freed and the corresponding memory is allocated for a different one. The stale reference is retained during event handler execution because of the `srcset` attribute which initially tries to load the image from the worng path.

Due to the code in the rest of the event handler, by the time the object is reused , it's memory has been populated by an object created with `new Image()`. In other words, `new Image()` ends up being allocated in the space that was occupied by the static element with id `html_image`.

```
#0 0x1ed3aa7c8 in WebCore::ImageLoader::dispatchPendingErrorEvent()+0x1e8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c67c8)
#1 0x1ed3aa4e4 in WebCore::ImageLoader::dispatchPendingEvent(WebCore::EventSender<WebCore::ImageLoader>*)+0x74
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c64e4)
#2 0x1ed3aa89a in WebCore::EventSender<WebCore::ImageLoader>::dispatchPendingEvents(WebCore::Page*)+0x7a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c689a)
#3 0x1ed3b254a in WebCore::EventSender<WebCore::ImageLoader>::timerFired()+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43ce54a)
```

Function `WebCore::ImageLoader::~ImageLoader()` should check if there are any pending operation on the object before freeing it.

By this point the objects that were used by event are deallocated, which can be seen by backtrace from the attached crash log.

```
#4 0x2089e4650 in bmalloc::api::free(void*, bmalloc::HeapKind)+0x10
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54650)
#5 0x2089e463a in WTF::fastFree(void*)+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x5463a)
#6 0x1ecaf9fd8 in WebCore::ImageLoader::operator delete(void*)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15fd8)
#7 0x1ecaf9faa in std::__1::default_delete<WebCore::HTMLImageLoader>::operator()(WebCore::HTMLImageLoader*) const+0x1a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15faa)
#8 0x1ecaf9f5c in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader>
>::reset(WebCore::HTMLImageLoader*)+0x3c (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15f5c)
#9 0x1ecaf9f18 in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15f18)
#10 0x1ecae81e8 in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b041e8)
#11 0x1ecae806a in WebCore::HTMLImageElement::~HTMLImageElement()+0x10a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0406a)
#12 0x1ecae81f8 in WebCore::HTMLImageElement::~HTMLImageElement()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b041f8)
#13 0x1ecae821d in WebCore::HTMLImageElement::~HTMLImageElement()+0xd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0421d)
#14 0x1ec6c2c93 in WebCore::Node::removedLastRef()+0x73
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x36dec93)
#15 0x1ebdd21ca in WTF::RefPtr<WebCore::Element, WTF::RawPtrTraits<WebCore::Element>, WTF::DefaultRefDerefTraits<WebCore::Element>
>::operator=(std::nullptr_t)+0x4a (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x2dee1ca)
```

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

Crash Information

```
==40816==ERROR: AddressSanitizer: heap-use-after-free on address 0x60b00003a018 at pc 0x0006b33467c9 bp 0x7ffee10572f0 sp 0x7ffee10572e8
READ of size 1 at 0x60b00003a018 thread T0
==40816==WARNING: invalid path to external symbolizer!
==40816==WARNING: Failed to use and restart external symbolizer!
    #0 0x6b33467c8 in WebCore::ImageLoader::dispatchPendingErrorEvent()+0x1e8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c67c8)
    #1 0x6b33464e4 in WebCore::ImageLoader::dispatchPendingEvent(WebCore::EventSender<WebCore::ImageLoader>*)+0x74
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c64e4)
    #2 0x6b334689a in WebCore::EventSender<WebCore::ImageLoader>::dispatchPendingEvents(WebCore::Page*)+0x7a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c689a)
    #3 0x6b334e54a in WebCore::EventSender<WebCore::ImageLoader>::timerFired()+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43ce54a)
    #4 0x6b334ed24 in decltype(*(std::__1::forward<WebCore::EventSender<WebCore::ImageLoader>*&>(fp0)).*fp()) std::__1::__invoke<void
(WebCore::EventSender<WebCore::ImageLoader>::*&)(), WebCore::EventSender<WebCore::ImageLoader>*&, void>(void
(WebCore::EventSender<WebCore::ImageLoader>::*&)(), WebCore::EventSender<WebCore::ImageLoader>*&)+0x84
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43ced24)
    #5 0x6b334ec93 in std::__1::__bind_return<void (WebCore::EventSender<WebCore::ImageLoader>::*)(),
std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>, std::__1::tuple<>, __is_valid_bind_return<void
(WebCore::EventSender<WebCore::ImageLoader>::*)(), std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>, std::__1::tuple<>
>::value>::type std::__1::__apply_functor<void (WebCore::EventSender<WebCore::ImageLoader>::*)(),
std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>, 0ul, std::__1::tuple<> >(void (WebCore::EventSender<WebCore::ImageLoader>::*&)
(), std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>&, std::__1::__tuple_indices<0ul>, std::__1::tuple<>&&)+0x23
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43cec93)
    #6 0x6b334ec6c in std::__1::__bind_return<void (WebCore::EventSender<WebCore::ImageLoader>::*)(),
std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>, std::__1::tuple<>, __is_valid_bind_return<void
(WebCore::EventSender<WebCore::ImageLoader>::*)(), std::__1::tuple<WebCore::EventSender<WebCore::ImageLoader>*>, std::__1::tuple<>
>::value>::type std::__1::__bind<void (WebCore::EventSender<WebCore::ImageLoader>::*&)(),
WebCore::EventSender<WebCore::ImageLoader>*>::operator()<>()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43cec6c)
    #7 0x6b334ec4c in WTF::Detail::CallableWrapper<std::__1::__bind<void (WebCore::EventSender<WebCore::ImageLoader>::*&)(),
WebCore::EventSender<WebCore::ImageLoader>*>, void>::call()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43cec4c)
    #8 0x6aef9647e in WTF::Function<void ()>::operator()() const+0x3e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1647e)
    #9 0x6aefd61ec in WebCore::Timer::fired()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x561ec)
    #10 0x6b3869b14 in WebCore::ThreadTimers::sharedTimerFiredInternal()+0x3a4
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48e9b14)
    #11 0x6b3875e38 in WebCore::ThreadTimers::setSharedTimer(WebCore::SharedTimer*)::$_0::operator()() const+0x18
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48f5e38)
    #12 0x6b3875e08 in WTF::Detail::CallableWrapper<WebCore::ThreadTimers::setSharedTimer(WebCore::SharedTimer*)::$_0, void>::call()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48f5e08)
    #13 0x6aef9647e in WTF::Function<void ()>::operator()() const+0x3e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1647e)
    #14 0x6b3817dfc in WebCore::MainThreadSharedTimer::fired()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4897dfc)
    #15 0x6b38ecdc9 in WebCore::timerFired(__CFRunLoopTimer*, void*)+0xb9
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x496cdc9)
    #16 0x7fff204368fc in __CFRUNLOOP_IS_CALLING_OUT_TO_A_TIMER_CALLBACK_FUNCTION__+0x13
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x9a8fc)
    #17 0x7fff204363d7 in __CFRunLoopDoTimer+0x399
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x9a3d7)
    #18 0x7fff20435f31 in __CFRunLoopDoTimers+0x132
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x99f31)
    #19 0x7fff2041c56e in __CFRunLoopRun+0x7d7
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x8056e)
    #20 0x7fff2041b6bd in CFRunLoopRunSpecific+0x232
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x7f6bd)
    #21 0x7fff211a5fa0 in -[NSRunLoop(NSRunLoop) runMode:beforeDate:]+0xd3
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0x5ffa0)
    #22 0x7fff21234383 in -[NSRunLoop(NSRunLoop) run]+0x4b
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0xee383)
    #23 0x7fff200753dc in _xpc_objc_main+0x338 (/usr/lib/system/libxpc.dylib:x86_64+0x153dc)
    #24 0x7fff20074e64 in xpc_main+0x1b4 (/usr/lib/system/libxpc.dylib:x86_64+0x14e64)
    #25 0x6a0e40a7f in WebKit::XPCServiceMain(int, char const**)+0x47f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0xe40a7f)
    #26 0x6a26f1f48 in WKXPCServiceMain+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x26f1f48)
    #27 0x10eba9e18 in main+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/com.apple.WebKit.WebContent.xpc/Contents/MacOS/com.apple.WebKit.WebContent.Development:x86_64+0
x100003e18)
    #28 0x7fff20340630 in start+0x0 (/usr/lib/system/libdyld.dylib:x86_64+0x15630)

0x60b00003a018 is located 104 bytes inside of 112-byte region [0x60b000039fb0,0x60b00003a020)
freed by thread T0 here:
    #0 0x6ad2a9dd6 in __sanitizer_mz_free+0x86
(/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/lib/clang/12.0.0/lib/darwin/libclang_rt.asan_osx_dynamic
.dylib:x86_64h+0x49dd6)
    #1 0x6ceafe9d4 in bmalloc::DebugHeap::free(void*)+0x24
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d29d4)
    #2 0x6ceafc548 in bmalloc::Cache::deallocateSlowCaseNullCache(bmalloc::HeapKind, void*)+0x68
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d0548)
    #3 0x6ce9811dd in bmalloc::Cache::deallocate(bmalloc::HeapKind, void*)+0x7d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x551dd)
    #4 0x6ce980650 in bmalloc::api::free(void*, bmalloc::HeapKind)+0x10
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54650)
    #5 0x6ce98063a in WTF::fastFree(void*)+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x5463a)
    #6 0x6b2a95fd8 in WebCore::ImageLoader::operator delete(void*)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15fd8)
    #7 0x6b2a95faa in std::__1::default_delete<WebCore::HTMLImageLoader>::operator()(WebCore::HTMLImageLoader*) const+0x1a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15faa)
    #8 0x6b2a95f5c in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader>
>::reset(WebCore::HTMLImageLoader*)+0x3c (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15f5c)
    #9 0x6b2a95f18 in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader> >::~unique_ptr()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b15f18)
    #10 0x6b2a841e8 in std::__1::unique_ptr<WebCore::HTMLImageLoader, std::__1::default_delete<WebCore::HTMLImageLoader>
>::~unique_ptr()+0x8 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b041e8)
    #11 0x6b2a8406a in WebCore::HTMLImageElement::~HTMLImageElement()+0x10a
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0406a)
    #12 0x6b2a841f8 in WebCore::HTMLImageElement::~HTMLImageElement()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b041f8)
    #13 0x6b2a8421d in WebCore::HTMLImageElement::~HTMLImageElement()+0xd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0421d)
    #14 0x6b265ec93 in WebCore::Node::removedLastRef()+0x73
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x36dec93)
    #15 0x6b1d6e1ca in WTF::RefPtr<WebCore::Element, WTF::RawPtrTraits<WebCore::Element>, WTF::DefaultRefDerefTraits<WebCore::Element>
>::operator=(std::nullptr_t)+0x4a (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x2dee1ca)
    #16 0x6b334382e in WebCore::ImageLoader::timerFired()+0xe
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c382e)
    #17 0x6b3362c34 in decltype(*(std::__1::forward<WebCore::ImageLoader*&>(fp0)).*fp()) std::__1::__invoke<void (WebCore::ImageLoader::*&)
(), WebCore::ImageLoader*&, void>(void (WebCore::ImageLoader::*&)(), WebCore::ImageLoader*&)+0x84
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43e2c34)
```

```
    #18 0x6b3362ba3 in std::__1::__bind_return<void (WebCore::ImageLoader::*)(), std::__1::tuple<WebCore::ImageLoader*>, std::__1::tuple<>,
__is_valid_bind_return<void (WebCore::ImageLoader::*)(), std::__1::tuple<WebCore::ImageLoader*>, std::__1::tuple<> >::value>::type
std::__1::__apply_functor<void (WebCore::ImageLoader::*)(), std::__1::tuple<WebCore::ImageLoader*>, 0ul, std::__1::tuple<> >(void
(WebCore::ImageLoader::*&)(), std::__1::tuple<WebCore::ImageLoader*>&, std::__1::__tuple_indices<0ul>, std::__1::tuple<>&&)+0x23
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43e2ba3)
    #19 0x6b3362b7c in std::__1::__bind_return<void (WebCore::ImageLoader::*)(), std::__1::tuple<WebCore::ImageLoader*>, std::__1::tuple<>,
__is_valid_bind_return<void (WebCore::ImageLoader::*)(), std::__1::tuple<WebCore::ImageLoader*>, std::__1::tuple<> >::value>::type
std::__1::__bind<void (WebCore::ImageLoader::*&)(), WebCore::ImageLoader*>::operator()<>()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43e2b7c)
    #20 0x6b3362b5c in WTF::Detail::CallableWrapper<std::__1::__bind<void (WebCore::ImageLoader::*&)(), WebCore::ImageLoader*>,
void>::call()+0xc (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43e2b5c)
    #21 0x6aef9647e in WTF::Function<void ()>::operator()() const+0x3e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1647e)
    #22 0x6aefd61ec in WebCore::Timer::fired()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x561ec)
    #23 0x6b3869b14 in WebCore::ThreadTimers::sharedTimerFiredInternal()+0x3a4
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48e9b14)
    #24 0x6b3875e38 in WebCore::ThreadTimers::setSharedTimer(WebCore::SharedTimer*)::$_0::operator()() const+0x18
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48f5e38)
    #25 0x6b3875e08 in WTF::Detail::CallableWrapper<WebCore::ThreadTimers::setSharedTimer(WebCore::SharedTimer*)::$_0, void>::call()+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x48f5e08)
    #26 0x6aef9647e in WTF::Function<void ()>::operator()() const+0x3e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x1647e)
    #27 0x6b3817dfc in WebCore::MainThreadSharedTimer::fired()+0xc
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4897dfc)
    #28 0x6b38ecdc9 in WebCore::timerFired(__CFRunLoopTimer*, void*)+0xb9
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x496cdc9)
    #29 0x7fff204368fc in __CFRUNLOOP_IS_CALLING_OUT_TO_A_TIMER_CALLBACK_FUNCTION__+0x13
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x9a8fc)

previously allocated by thread T0 here:
    #0 0x6ad2a99dd in __sanitizer_mz_malloc+0x9d
(/Applications/Xcode.app/Contents/Developer/Toolchains/XcodeDefault.xctoolchain/usr/lib/clang/12.0.0/lib/darwin/libclang_rt.asan_osx_dynamic
.dylib:x86_64h+0x499dd)
    #1 0x7fff20165dfd in _malloc_zone_malloc+0x75 (/usr/lib/system/libsystem_malloc.dylib:x86_64+0x1bdfd)
    #2 0x6ceafe8e8 in bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)+0x28
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d28e8)
    #3 0x6ceafc290 in bmalloc::Cache::allocateSlowCaseNullCache(bmalloc::HeapKind, unsigned long)+0x70
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x1d0290)
    #4 0x6ce980d0d in bmalloc::Cache::allocate(bmalloc::HeapKind, unsigned long)+0x7d
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54d0d)
    #5 0x6ce980440 in bmalloc::api::malloc(unsigned long, bmalloc::HeapKind)+0x10
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x54440)
    #6 0x6ce9801ca in WTF::fastMalloc(unsigned long)+0xa
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/JavaScriptCore.framework/Versions/A/JavaScriptCore:x86_64+0x541ca)
    #7 0x6b2a8ce58 in WebCore::ImageLoader::operator new(unsigned long)+0x8
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0ce58)
    #8 0x6b2a8ce09 in std::__1::__unique_if<WebCore::HTMLImageLoader>::__unique_single std::__1::make_unique<WebCore::HTMLImageLoader,
WebCore::HTMLImageElement&>(WebCore::HTMLImageElement&)+0x19
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b0ce09)
    #9 0x6b2a83cc2 in WebCore::HTMLImageElement::HTMLImageElement(WebCore::QualifiedName const&, WebCore::Document&,
WebCore::HTMLFormElement*)+0x82 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b03cc2)
    #10 0x6b2a83e98 in WebCore::HTMLImageElement::HTMLImageElement(WebCore::QualifiedName const&, WebCore::Document&,
WebCore::HTMLFormElement*)+0x8 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b03e98)
    #11 0x6b2a83f37 in WebCore::HTMLImageElement::create(WebCore::QualifiedName const&, WebCore::Document&, WebCore::HTMLFormElement*)+0x37
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3b03f37)
    #12 0x6af41a02d in WebCore::imageConstructor(WebCore::QualifiedName const&, WebCore::Document&, WebCore::HTMLFormElement*, bool)+0xbd
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x49a02d)
    #13 0x6af4156b1 in WebCore::HTMLElementFactory::createKnownElement(WTF::AtomString const&, WebCore::Document&,
WebCore::HTMLFormElement*, bool)+0xe1 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x4956b1)
    #14 0x6b2db3353 in WebCore::HTMLConstructionSite::createHTMLElementOrFindCustomElementInterface(WebCore::AtomicHTMLToken&,
WebCore::JSCustomElementInterface**)+0x133
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e33353)
    #15 0x6b2db234a in WebCore::HTMLConstructionSite::createHTMLElement(WebCore::AtomicHTMLToken&)+0xba
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e3234a)
    #16 0x6b2db3be0 in WebCore::HTMLConstructionSite::insertSelfClosingHTMLElement(WebCore::AtomicHTMLToken&&)+0xe0
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e33be0)
    #17 0x6b2e0bf24 in WebCore::HTMLTreeBuilder::processStartTagForInBody(WebCore::AtomicHTMLToken&&)+0x1444
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e8bf24)
    #18 0x6b2e08281 in WebCore::HTMLTreeBuilder::processStartTag(WebCore::AtomicHTMLToken&&)+0x1b01
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e88281)
    #19 0x6b2e0648e in WebCore::HTMLTreeBuilder::processToken(WebCore::AtomicHTMLToken&&)+0x17e
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e8648e)
    #20 0x6b2e054b2 in WebCore::HTMLTreeBuilder::constructTree(WebCore::AtomicHTMLToken&&)+0x42
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e854b2)
    #21 0x6b2db8f25 in WebCore::HTMLDocumentParser::constructTreeFromHTMLToken(WebCore::HTMLTokenizer::TokenPtr&)+0x135
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e38f25)
    #22 0x6b2db8886 in WebCore::HTMLDocumentParser::pumpTokenizerLoop(WebCore::HTMLDocumentParser::SynchronousMode, bool,
WebCore::PumpSession&)+0x176 (/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e38886)
    #23 0x6b2db7a39 in WebCore::HTMLDocumentParser::pumpTokenizer(WebCore::HTMLDocumentParser::SynchronousMode)+0x169
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e37a39)
    #24 0x6b2db7625 in WebCore::HTMLDocumentParser::pumpTokenizerIfPossible(WebCore::HTMLDocumentParser::SynchronousMode)+0x65
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e37625)
    #25 0x6b2db9ab6 in WebCore::HTMLDocumentParser::append(WTF::RefPtr<WTF::StringImpl, WTF::RawPtrTraits<WTF::StringImpl>,
WTF::DefaultRefDerefTraits<WTF::StringImpl> >&&)+0x336
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x3e39ab6)
    #26 0x6b248fb02 in WebCore::DecodedDataDocumentParser::appendBytes(WebCore::DocumentWriter&, char const*, unsigned long)+0x152
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x350fb02)
    #27 0x6b32ec838 in WebCore::DocumentWriter::addData(char const*, unsigned long)+0x78
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x436c838)
    #28 0x6b329d8ff in WebCore::DocumentLoader::commitData(char const*, unsigned long)+0x38f
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x431d8ff)
    #29 0x6a20c248d in WebKit::WebFrameLoaderClient::committedLoad(WebCore::DocumentLoader*, char const*, int)+0xed
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebKit.framework/Versions/A/WebKit:x86_64+0x20c248d)

SUMMARY: AddressSanitizer: heap-use-after-free
(/Users/mt/Fuzzer/WebKit/WebKitBuild/Release/WebCore.framework/Versions/A/WebCore:x86_64+0x43c67c8) in
WebCore::ImageLoader::dispatchPendingErrorEvent()+0x1e8
Shadow bytes around the buggy address:
  0x1c16000073b0: fa fa fa fa 00 00 00 00 00 00 00 00 00 00 00 00
  0x1c16000073c0: 00 00 fa fa fa fa fa fa fa fa fd fd fd fd fd fd
  0x1c16000073d0: fd fd fd fd fd fd fd fd fa fa fa fa fa fa fa fa
  0x1c16000073e0: fd fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa
  0x1c16000073f0: fa fa fa fa fa fa fd fd fd fd fd fd fd fd fd fd
=>0x1c1600007400: fd fd fd[fd]fa fa fa fa fa fa fa fa fd fd fd fd
  0x1c1600007410: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x1c1600007420: fa fa fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c1600007430: fa fa fa fa fa fa fa fa fd fd fd fd fd fd fd fd
  0x1c1600007440: fd fd fd fd fd fd fd fa fa fa fa fa fa fa fd fd
  0x1c1600007450: fd fd fd fd fd fd fd fd fd fd fd fd 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
==40816==ABORTING
2021-01-11 10:13:29.934 MiniBrowser[40812:8062928] WebContent process crashed; reloading
```

Timeline

2021-01-21 - Vendor Disclosure

2021-03-15 - Vendor Patched

2021-06-02 - Public Release

CREDIT

Discovered by Marcin Towalski of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1142

NEXT REPORT TALOS-2021-1246