master security_advisories / webkitgtk-2.36.0 /

ChijinZ update webkit … on May 5 History

..

poc	7 months ago
readme.md	7 months ago

readme.md

heap-buffer-overflow in WebCore::TextureMapperLayer::setContentsLayer

report id: Bug 237187

The attached file cause a heap buffer overflow in setContentsLayer().

version: webkitgtk 2.36.0

ASan report:

```
==16712==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x61b0000d4ab8
at pc 0x7f79a33b83ff bp 0x7ffde8451be0 sp 0x7ffde8451bd8 WRITE of size 8 at
0x61b0000d4ab8 thread T0 #0 0x7f79a33b83fe in
WebCore::TextureMapperLayer::setContentsLayer(WebCore::TextureMapperPlatformLayer*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperLayer.cpp:702:21 #1
0x7f79a33d29aa in
WebCore::TextureMapperPlatformLayerProxy::~TextureMapperPlatformLayerProxy()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperPlatformLayerProxy.cp
p:56:24 #2 0x7f79a33d2ed8 in
WebCore::TextureMapperPlatformLayerProxy::~TextureMapperPlatformLayerProxy()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperPlatformLayerProxy.cp
p:53:1 #3 0x7f79a3410b9f in
WTF::ThreadSafeRefCounted<WebCore::TextureMapperPlatformLayerProxy,
(WTF::DestructionThread)0>::deref() const::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:117:13 #4 0x7f79a3410b9f in
WTF::ThreadSafeRefCounted<WebCore::TextureMapperPlatformLayerProxy,
(WTF::DestructionThread)0>::deref() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:129:9 #5 0x7f79a3410b9f in
WTF::Ref<WebCore::TextureMapperPlatformLayerProxy,
WTF::RawPtrTraitsWebCore::TextureMapperPlatformLayerProxy >::~Ref()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/Ref.h:61:18 #6
0x7f79a3410b9f in
Nicosia::ContentLayerTextureMapperImpl::~ContentLayerTextureMapperImpl()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaContentLayerTextureM
apperImpl.cpp:58:1 #7 0x7f79a3410c48 in
Nicosia::ContentLayerTextureMapperImpl::~ContentLayerTextureMapperImpl()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaContentLayerTextureM
apperImpl.cpp:53:1 #8 0x7f79a34061ab in
std::default_deleteNicosia::ContentLayer::Impl::operator()(Nicosia::ContentLayer::Impl*)
const /usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #9
```

```
0x7f79a34061ab in std::unique_ptr<Nicosia::ContentLayer::Impl,
std::default_deleteNicosia::ContentLayer::Impl >::~unique_ptr() /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:292:4 #10 0x7f79a34061ab in
Nicosia::ContentLayer::~ContentLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/NicosiaPlatformLayer.cpp:58:29 #11
0x7f79a3406388 in Nicosia::ContentLayer::~ContentLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/NicosiaPlatformLayer.cpp:58:29 #12
0x7f79a9447ea2 in WTF::ThreadSafeRefCounted<Nicosia::PlatformLayer,
(WTF::DestructionThread)0>::deref() const::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:117:13 #13 0x7f79a9447ea2 in
WTF::ThreadSafeRefCounted<Nicosia::PlatformLayer, (WTF::DestructionThread)0>::deref()
const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:129:9 #14 0x7f79a9447ea2 in WTF::Ref<Nicosia::ContentLayer,
WTF::RawPtrTraitsNicosia::ContentLayer >::~Ref()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/Ref.h:61:18 #15
0x7f79a9447ea2 in Nicosia::GCGLLayer::~GCGLLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaGCGLLayer.cpp:60:1
#16 0x7f79a9447fa8 in Nicosia::GCGLLayer::~GCGLLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaGCGLLayer.cpp:58:1
#17 0x7f79a94201f2 in std::default_deleteNicosia::GCGLLayer::operator()
(Nicosia::GCGLLayer*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #18 0x7f79a94201f2 in
std::unique_ptr<Nicosia::GCGLLayer, std::default_deleteNicosia::GCGLLayer >::~unique_ptr()
/usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:292:4 #19
0x7f79a94201f2 in WebCore::GraphicsContextGLOpenGL::~GraphicsContextGLOpenGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/GraphicsContextGLTextureMapper.cpp
:386:1 #20 0x7f79a9420918 in
WebCore::GraphicsContextGLOpenGL::~GraphicsContextGLOpenGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/GraphicsContextGLTextureMapper.cpp
:348:1 #21 0x7f79a6a9d7be in std::default_deleteWebCore::GraphicsContextGL::operator()
```

```
(WebCore::GraphicsContextGL*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #22 0x7f79a6a9d7be in
WTF::RefCounted<WebCore::GraphicsContextGL,
std::default_deleteWebCore::GraphicsContextGL >::deref() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefCounted.h:19
0:13 #23 0x7f79a6a9d7be in
WTF::DefaultRefDerefTraitsWebCore::GraphicsContextGL::derefIfNotNull(WebCore::Graphics
ContextGL*) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#24 0x7f79a6a9d7be in WTF::RefPtr<WebCore::GraphicsContextGL,
WTF::RawPtrTraitsWebCore::GraphicsContextGL,
WTF::DefaultRefDerefTraitsWebCore::GraphicsContextGL >::operator=(std::nullptr_t)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:159:5
#25 0x7f79a6a9d7be in
WebCore::WebGLRenderingContextBase::destroyGraphicsContextGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContextBase.cpp:1199:19 #26
0x7f79a6ae593a in
WebCore::WebGLRenderingContextBase::~WebGLRenderingContextBase()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContextBase.cpp:1174:9 #27
0x7f79a6afbe1f in WebCore::WebGLRenderingContext::~WebGLRenderingContext()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContext.h:35:7 #28 0x7f79a6afbe1f
in non-virtual thunk to WebCore::WebGLRenderingContext::~WebGLRenderingContext()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContext.h #29 0x7f79a65cbef4 in
std::default_deleteWebCore::CanvasRenderingContext::operator()
(WebCore::CanvasRenderingContext*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #30 0x7f79a65cbef4 in
std::unique_ptr<WebCore::CanvasRenderingContext,
std::default_deleteWebCore::CanvasRenderingContext
>::reset(WebCore::CanvasRenderingContext*) /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:402:4 #31 0x7f79a65cbef4 in
std::unique_ptr<WebCore::CanvasRenderingContext,
std::default_deleteWebCore::CanvasRenderingContext >::operator=(std::nullptr_t)
/usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:336:2 #32
0x7f79a65cbef4 in WebCore::HTMLCanvasElement::~HTMLCanvasElement()
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLCanvasElement.cpp:148:15 #33 0x7f79a65cc668 in
WebCore::HTMLCanvasElement::~HTMLCanvasElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLCanvasElement.cpp:141:1 #34 0x7f79a5db5577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #35 0x7f79a5db5577 in
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#36 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#37 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#38 0x7f79a5db5577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #39 0x7f79a5d9b84e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #40 0x7f79a5d9b84e
in WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #41 0x7f79a5d9d665 in
WebCore::ContainerNode::~ContainerNode()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:316:5 #42 0x7f79a65c6518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #43 0x7f79a65c6518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #44 0x7f79a5db5577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #45 0x7f79a5db5577 in
```

```
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#46 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#47 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#48 0x7f79a5db5577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #49 0x7f79a5d9b84e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #50 0x7f79a5d9b84e
in WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #51 0x7f79a5d9d665 in
WebCore::ContainerNode::~ContainerNode()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:316:5 #52 0x7f79a666d2d8 in
WebCore::HTMLHtmlElement::~HTMLHtmlElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLHtmlElement.h:30:7 #53 0x7f79a5db5577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #54 0x7f79a5db5577 in
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#55 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#56 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#57 0x7f79a5db5577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #58 0x7f79a5d9b84e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #59 0x7f79a5d9b84e
in WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #60 0x7f79a5d9d665 in
WebCore::ContainerNode::~ContainerNode()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:316:5 #61 0x7f79a65c6518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #62 0x7f79a65c6518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #63 0x7f79a5db5577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #64 0x7f79a5db5577 in
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#65 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#66 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#67 0x7f79a5db5577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #68 0x7f79a5d9b84e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #69 0x7f79a5d9b84e
in WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #70 0x7f79a5d9d665 in
WebCore::ContainerNode::~ContainerNode()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:316:5 #71 0x7f79a666d2d8 in
WebCore::HTMLHtmlElement::~HTMLHtmlElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLHtmlElement.h:30:7 #72 0x7f79a5db5577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #73 0x7f79a5db5577 in
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#74 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#75 0x7f79a5db5577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#76 0x7f79a5db5577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #77 0x7f79a5d9b84e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #78 0x7f79a5d9b84e
in WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #79 0x7f79a5e19b07 in
WebCore::Document::removedLastRef()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Document.cpp:822:9 #80 0x7f79a65daabc in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #81 0x7f79a65daabc in
```

```
WTF::Ref<WebCore::ContainerNode, WTF::RawPtrTraitsWebCore::ContainerNode >::~Ref()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/Ref.h:61:18 #82
0x7f79a65daabc in WebCore::HTMLCollection::~HTMLCollection()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLCollection.cpp:143:1 #83 0x7f79a5f02a59 in
WebCore::CachedHTMLCollection<WebCore::GenericCachedHTMLCollection<(WebCore::C
ollectionTraversalType)0>,
(WebCore::CollectionTraversalType)0>::~CachedHTMLCollection()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/CachedHTMLCollection.h:85:1 #84 0x7f79a5f02b78 in
WebCore::GenericCachedHTMLCollection<(WebCore::CollectionTraversalType)0>::~Generic
CachedHTMLCollection() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/GenericCachedHTMLCollection.h:33:7 #85 0x7f799df2bd84
in JSC::JSDestructibleObjectDestroyFunc::operator()(JSC::VM&, JSC::JSCell*) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:38:9 #86
0x7f799df2bd84 in void JSC::MarkedBlock::Handle::specializedSweep<true,
(JSC::MarkedBlock::Handle::EmptyMode)0, (JSC::MarkedBlock::Handle::SweepMode)1,
(JSC::MarkedBlock::Handle::SweepDestructionMode)1,
(JSC::MarkedBlock::Handle::ScribbleMode)0,
(JSC::MarkedBlock::Handle::NewlyAllocatedMode)1,
(JSC::MarkedBlock::Handle::MarksMode)0, JSC::JSDestructibleObjectDestroyFunc>
(JSC::FreeList*, JSC::MarkedBlock::Handle::EmptyMode,
JSC::MarkedBlock::Handle::SweepMode, JSC::MarkedBlock::Handle::SweepDestructionMode,
JSC::MarkedBlock::Handle::ScribbleMode, JSC::MarkedBlock::Handle::NewlyAllocatedMode,
JSC::MarkedBlock::Handle::MarksMode, JSC::JSDestructibleObjectDestroyFunc
const&)::'lambda'(void*)::operator()(void*) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedBlockInlines.h:260:13 #87 0x7f799df2bd84 in
void JSC::MarkedBlock::Handle::specializedSweep<true,
(JSC::MarkedBlock::Handle::EmptyMode)0, (JSC::MarkedBlock::Handle::SweepMode)1,
(JSC::MarkedBlock::Handle::SweepDestructionMode)1,
(JSC::MarkedBlock::Handle::ScribbleMode)0,
(JSC::MarkedBlock::Handle::NewlyAllocatedMode)1,
(JSC::MarkedBlock::Handle::MarksMode)0, JSC::JSDestructibleObjectDestroyFunc>
(JSC::FreeList*, JSC::MarkedBlock::Handle::EmptyMode,
JSC::MarkedBlock::Handle::SweepMode, JSC::MarkedBlock::Handle::SweepDestructionMode,
JSC::MarkedBlock::Handle::ScribbleMode, JSC::MarkedBlock::Handle::NewlyAllocatedMode,
JSC::MarkedBlock::Handle::MarksMode, JSC::JSDestructibleObjectDestroyFunc const&)
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedBlockInlines.h:294:17 #88 0x7f799df265d1 in
void
JSC::MarkedBlock::Handle::finishSweepKnowingHeapCellTypeJSC::JSDestructibleObjectDestr
oyFunc(JSC::FreeList*, JSC::JSDestructibleObjectDestroyFunc const&)::'lambda'()::operator()()
const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedBlockInlines.h:403:21 #89 0x7f799df16158 in
void
JSC::MarkedBlock::Handle::finishSweepKnowingHeapCellTypeJSC::JSDestructibleObjectDestr
oyFunc(JSC::FreeList*, JSC::JSDestructibleObjectDestroyFunc const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedBlockInlines.h:435:9 #90 0x7f799df049b8 in
JSC::JSDestructibleObjectHeapCellType::finishSweep(JSC::MarkedBlock::Handle&,
JSC::FreeList*) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSDestructibleObjectHeapCellType.cpp:53:12 #91
0x7f799cdb19d9 in JSC::MarkedBlock::Handle::sweep(JSC::FreeList*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedBlock.cpp:415:21 #92 0x7f799cd9d31f in
JSC::LocalAllocator::tryAllocateIn(JSC::MarkedBlock::Handle*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocator.cpp:225:12 #93 0x7f799cd9d0fa in
JSC::LocalAllocator::tryAllocateWithoutCollecting()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocator.cpp:191:28 #94 0x7f799cd9c662 in
JSC::LocalAllocator::allocateSlowCase(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocator.cpp:132:20 #95 0x7f79a53ee008 in
JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode)::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/LocalAllocatorInlines.h:40:43 #96 0x7f79a53ee008 in JSC::HeapCell*
JSC::FreeList::allocate<JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode)::'lambda'()>(JSC::LocalAllocator::allocate(JSC::Heap&,
JSC::GCDeferralContext*, JSC::AllocationFailureMode)::'lambda'() const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/FreeListInlines.h:46:16 #97 0x7f79a53ee008 in
JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
```

```
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/LocalAllocatorInlines.h:37:23 #98 0x7f79a53ee008 in
JSC::Allocator::allocate(JSC::Heap&, JSC::GCDeferralContext*, JSC::AllocationFailureMode)
const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/AllocatorInlines.h:35:30 #99 0x7f79a53ee008 in
JSC::IsoSubspace::allocateNonVirtual(JSC::VM&, unsigned long, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/IsoSubspaceInlines.h:34:30 #100 0x7f79a53ee008 in void*
JSC::tryAllocateCellHelperWebCore::JSHTMLCollection(JSC::Heap&, unsigned long,
JSC::GCDeferralContext*, JSC::AllocationFailureMode)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/JSCellInlines.h:180:63 #101 0x7f79a53ee008 in void*
JSC::allocateCellWebCore::JSHTMLCollection(JSC::Heap&, unsigned long)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/JavaScriptCore/PrivateHeaders/Java
ScriptCore/JSCellInlines.h:194:12 #102 0x7f79a53e97f3 in
WebCore::JSHTMLCollection::create(JSC::Structure*, WebCore::JSDOMGlobalObject*,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/DerivedSources/JSHTMLC
ollection.h:34:47 #103 0x7f79a53e97f3 in
std::enable_if<std::is_same<WebCore::HTMLCollection, WebCore::HTMLCollection>::value,
WebCore::JSDOMWrapperConverterTraitsWebCore::HTMLCollection::WrapperClass*>::type
WebCore::createWrapper<WebCore::HTMLCollection, WebCore::HTMLCollection>
(WebCore::JSDOMGlobalObject*, WTF::Ref<WebCore::HTMLCollection,
WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMWrapperCache.h:190:21 #104 0x7f79a53e9caa
in WebCore::toJSNewlyCreated(JSC::JSGlobalObject*, WebCore::JSDOMGlobalObject*,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSHTMLCollectionCustom.cpp:45:12 #105
0x7f79a53e9caa in JSC::JSValue
WebCore::wrapWebCore::HTMLCollection(JSC::JSGlobalObject*,
WebCore::JSDOMGlobalObject*, WebCore::HTMLCollection&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMWrapperCache.h:204:12 #106 0x7f79a35c6e00
```

```
in JSC::JSValue WebCore::JSConverter<WebCore::IDLInterfaceWebCore::HTMLCollection
>::convert<WTF::Ref<WebCore::HTMLCollection,
WTF::RawPtrTraitsWebCore::HTMLCollection > >(JSC::JSGlobalObject&,
WebCore::JSDOMGlobalObject&, WTF::Ref<WebCore::HTMLCollection,
WTF::RawPtrTraitsWebCore::HTMLCollection > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMConvertInterface.h:81:16 #107
0x7f79a35c6e00 in JSC::JSValue
WebCore::JSConverterOverloader<WebCore::IDLInterfaceWebCore::HTMLCollection, true,
true>::convert<WTF::Ref<WebCore::HTMLCollection,
WTF::RawPtrTraitsWebCore::HTMLCollection > >(JSC::JSGlobalObject&,
WebCore::JSDOMGlobalObject&, WTF::Ref<WebCore::HTMLCollection,
WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMConvertBase.h:109:16 #108 0x7f79a35c6e00 in
JSC::JSValue WebCore::toJS<WebCore::IDLInterfaceWebCore::HTMLCollection,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection > >
(JSC::JSGlobalObject&, WebCore::JSDOMGlobalObject&,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMConvertBase.h:151:12 #109 0x7f79a35c6e00 in
JSC::JSValue WebCore::toJS<WebCore::IDLInterfaceWebCore::HTMLCollection,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection > >
(JSC::JSGlobalObject&, WebCore::JSDOMGlobalObject&, JSC::ThrowScope&,
WTF::Ref<WebCore::HTMLCollection, WTF::RawPtrTraitsWebCore::HTMLCollection >&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMConvertBase.h:215:20 #110 0x7f79a35c6e00 in
WebCore::jsDocumentPrototypeFunction_getElementsByTagNameBody(JSC::JSGlobalObject
*, JSC::CallFrame*, WebCore::JSDocument*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/DerivedSources/JSDocum
ent.cpp:5294:5 #111 0x7f79a35c6e00 in long
WebCore::IDLOperationWebCore::JSDocument::call<&
(WebCore::jsDocumentPrototypeFunction_getElementsByTagNameBody(JSC::JSGlobalObjec
t*, JSC::CallFrame*, WebCore::JSDocument*)), (WebCore::CastedThisErrorBehavior)0>
(JSC::JSGlobalObject&, JSC::CallFrame&, char const*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMOperation.h:63:9 #112 0x7f79a35c6e00 in
WebCore::jsDocumentPrototypeFunction_getElementsByTagName(JSC::JSGlobalObject*,
JSC::CallFrame*) /root/browser/webkit/webkit_trunck_clean_version/Safari-
```

branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/DerivedSources/JSDocument.cpp:5299:12 #113 0x7f7952feb1d7 ()

Address 0x61b0000d4ab8 is a wild pointer. SUMMARY: AddressSanitizer: heap-buffer-overflow /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/platform/graphics/texmap/TextureMapperLayer.cpp:702:21 in WebCore::TextureMapperLayer::setContentsLayer(WebCore::TextureMapperPlatformLayer*) Shadow bytes around the buggy address: 0x0c3680012900: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012910: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012920: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012930: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012940: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa =>0x0c3680012950: fa fa fa fa fa fa fa[fa]fa fa fa fa fa fa fa fa 0x0c3680012960: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012970: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012980: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c3680012990: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 0x0c36800129a0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa Shadow byte legend (one shadow byte represents 8 application bytes): Addressable: 00 Partially addressable: 01 02 03 04 05 06 07 Heap left redzone: fa Freed heap region: fd Stack left redzone: f1 Stack mid redzone: f2 Stack right redzone: f3 Stack after return: f5 Stack use after scope: f8 Global redzone: f9 Global init order: f6 Poisoned by user: f7 Container overflow: fc Array cookie: ac Intra object redzone: bb ASan internal: fe Left alloca redzone: ca Right alloca redzone: cb Shadow gap: cc ==16712==ABORTING

heap-use-after-free in setContentsLayer(WebCore::TextureMapperPlatformLayer*)

report id: Bug 237188

The attached file cause a heap use after free in setContentsLayer.

version: webkitgtk 2.36.0

ASan report:

```
==18385==ERROR: AddressSanitizer: heap-use-after-free on address 0x61b00012d7b8 at
pc 0x7f751aa143ff bp 0x7ffcc1bb1f80 sp 0x7ffcc1bb1f78 WRITE of size 8 at
0x61b00012d7b8 thread T0 #0 0x7f751aa143fe in
WebCore::TextureMapperLayer::setContentsLayer(WebCore::TextureMapperPlatformLayer*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperLayer.cpp:702:21 #1
0x7f751aa2e9aa in
WebCore::TextureMapperPlatformLayerProxy::~TextureMapperPlatformLayerProxy()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperPlatformLayerProxy.cp
p:56:24 #2 0x7f751aa2eed8 in
WebCore::TextureMapperPlatformLayerProxy::~TextureMapperPlatformLayerProxy()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperPlatformLayerProxy.cp
p:53:1 #3 0x7f751aa6cb9f in
WTF::ThreadSafeRefCounted<WebCore::TextureMapperPlatformLayerProxy,
(WTF::DestructionThread)0>::deref() const::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:117:13 #4 0x7f751aa6cb9f in
WTF::ThreadSafeRefCounted<WebCore::TextureMapperPlatformLayerProxy,
(WTF::DestructionThread)0>::deref() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:129:9 #5 0x7f751aa6cb9f in
WTF::Ref<WebCore::TextureMapperPlatformLayerProxy,
WTF::RawPtrTraitsWebCore::TextureMapperPlatformLayerProxy >::~Ref()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/Ref.h:61:18 #6
0x7f751aa6cb9f in
Nicosia::ContentLayerTextureMapperImpl::~ContentLayerTextureMapperImpl()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaContentLayerTextureM
apperImpl.cpp:58:1 #7 0x7f751aa6cc48 in
Nicosia::ContentLayerTextureMapperImpl::~ContentLayerTextureMapperImpl()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaContentLayerTextureM
apperImpl.cpp:53:1 #8 0x7f751aa621ab in
std::default_deleteNicosia::ContentLayer::Impl::operator()(Nicosia::ContentLayer::Impl*)
const /usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #9
```

```
0x7f751aa621ab in std::unique_ptr<Nicosia::ContentLayer::Impl,
std::default_deleteNicosia::ContentLayer::Impl >::~unique_ptr() /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:292:4 #10 0x7f751aa621ab in
Nicosia::ContentLayer::~ContentLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/NicosiaPlatformLayer.cpp:58:29 #11
0x7f751aa62388 in Nicosia::ContentLayer::~ContentLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/NicosiaPlatformLayer.cpp:58:29 #12
0x7f7520aa3ea2 in WTF::ThreadSafeRefCounted<Nicosia::PlatformLayer,
(WTF::DestructionThread)0>::deref() const::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:117:13 #13 0x7f7520aa3ea2 in
WTF::ThreadSafeRefCounted<Nicosia::PlatformLayer, (WTF::DestructionThread)0>::deref()
const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ThreadSafeRefCo
unted.h:129:9 #14 0x7f7520aa3ea2 in WTF::Ref<Nicosia::ContentLayer,
WTF::RawPtrTraitsNicosia::ContentLayer >::~Ref()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/Ref.h:61:18 #15
0x7f7520aa3ea2 in Nicosia::GCGLLayer::~GCGLLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaGCGLLayer.cpp:60:1
#16 0x7f7520aa3fa8 in Nicosia::GCGLLayer::~GCGLLayer()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/nicosia/texmap/NicosiaGCGLLayer.cpp:58:1
#17 0x7f7520a7c1f2 in std::default_deleteNicosia::GCGLLayer::operator()
(Nicosia::GCGLLayer*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #18 0x7f7520a7c1f2 in
std::unique_ptr<Nicosia::GCGLLayer, std::default_deleteNicosia::GCGLLayer >::~unique_ptr()
/usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:292:4 #19
0x7f7520a7c1f2 in WebCore::GraphicsContextGLOpenGL::~GraphicsContextGLOpenGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/GraphicsContextGLTextureMapper.cpp
:386:1 #20 0x7f7520a7c918 in
WebCore::GraphicsContextGLOpenGL::~GraphicsContextGLOpenGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/GraphicsContextGLTextureMapper.cpp
:348:1 #21 0x7f751e0f97be in std::default_deleteWebCore::GraphicsContextGL::operator()
```

```
(WebCore::GraphicsContextGL*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #22 0x7f751e0f97be in
WTF::RefCounted<WebCore::GraphicsContextGL,
std::default_deleteWebCore::GraphicsContextGL >::deref() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefCounted.h:19
0:13 #23 0x7f751e0f97be in
WTF::DefaultRefDerefTraitsWebCore::GraphicsContextGL::derefIfNotNull(WebCore::Graphics
ContextGL*) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#24 0x7f751e0f97be in WTF::RefPtr<WebCore::GraphicsContextGL,
WTF::RawPtrTraitsWebCore::GraphicsContextGL,
WTF::DefaultRefDerefTraitsWebCore::GraphicsContextGL >::operator=(std::nullptr_t)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:159:5
#25 0x7f751e0f97be in
WebCore::WebGLRenderingContextBase::destroyGraphicsContextGL()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContextBase.cpp:1199:19 #26
0x7f751e14193a in
WebCore::WebGLRenderingContextBase::~WebGLRenderingContextBase()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContextBase.cpp:1174:9 #27
0x7f751e157e1f in WebCore::WebGLRenderingContext::~WebGLRenderingContext()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContext.h:35:7 #28 0x7f751e157e1f
in non-virtual thunk to WebCore::WebGLRenderingContext::~WebGLRenderingContext()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/canvas/WebGLRenderingContext.h #29 0x7f751dc27ef4 in
std::default_deleteWebCore::CanvasRenderingContext::operator()
(WebCore::CanvasRenderingContext*) const /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:81:2 #30 0x7f751dc27ef4 in
std::unique_ptr<WebCore::CanvasRenderingContext,
std::default_deleteWebCore::CanvasRenderingContext
>::reset(WebCore::CanvasRenderingContext*) /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:402:4 #31 0x7f751dc27ef4 in
std::unique_ptr<WebCore::CanvasRenderingContext,
std::default_deleteWebCore::CanvasRenderingContext >::operator=(std::nullptr_t)
/usr/lib/gcc/x86_64-linux-gnu/9/../../../../include/c++/9/bits/unique_ptr.h:336:2 #32
0x7f751dc27ef4 in WebCore::HTMLCanvasElement::~HTMLCanvasElement()
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLCanvasElement.cpp:148:15 #33 0x7f751dc28668 in
WebCore::HTMLCanvasElement::~HTMLCanvasElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLCanvasElement.cpp:141:1 #34 0x7f751d411577 in
WebCore::Node::deref() const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/Node.h:804:34 #35 0x7f751d411577 in
WTF::DefaultRefDerefTraitsWebCore::Node::derefIfNotNull(WebCore::Node*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:42:18
#36 0x7f751d411577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::~RefPtr()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:73:31
#37 0x7f751d411577 in WTF::RefPtr<WebCore::Node, WTF::RawPtrTraitsWebCore::Node,
WTF::DefaultRefDerefTraitsWebCore::Node >::operator=(WTF::RefPtr<WebCore::Node,
WTF::RawPtrTraitsWebCore::Node, WTF::DefaultRefDerefTraitsWebCore::Node > const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/RefPtr.h:137:1
#38 0x7f751d411577 in WebCore::addChildNodesToDeletionQueue(WebCore::Node*&,
WebCore::Node*&, WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:186:65 #39 0x7f751d3f784e
in WebCore::removeDetachedChildrenInContainer(WebCore::ContainerNode&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNodeAlgorithms.cpp:225:5 #40 0x7f751d3f784e in
WebCore::ContainerNode::removeDetachedChildren()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:282:5 #41 0x7f751d3f9665 in
WebCore::ContainerNode::~ContainerNode()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/dom/ContainerNode.cpp:316:5 #42 0x7f751dc22518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #43 0x7f751dc22518 in
WebCore::HTMLBodyElement::~HTMLBodyElement()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/html/HTMLBodyElement.cpp:64:35 #44 0x7f751442eb3a in
JSC::PreciseAllocation::sweep() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/PreciseAllocation.cpp:234:25 #45 0x7f7514414ff8 in
```

```
JSC::MarkedSpace::sweepPreciseAllocations()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MarkedSpace.cpp:235:21 #46 0x7f7514387248 in
JSC::Heap::sweepInFinalize() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:2116:19 #47 0x7f7514387248 in
JSC::Heap::finalize() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:2061:9 #48 0x7f7514386195 in
JSC::Heap::handleNeedFinalize(unsigned int)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1997:9 #49 0x7f751437ac59 in
JSC::Heap::handleNeedFinalize() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:2008:12 #50 0x7f751437ac59 in
JSC::Heap::finishChangingPhase(JSC::GCConductor)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1604:17 #51 0x7f7514380ff0 in
JSC::Heap::changePhase(JSC::GCConductor, JSC::CollectorPhase)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1578:12 #52 0x7f7514380ff0 in
JSC::Heap::runEndPhase(JSC::GCConductor)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1568:12 #53 0x7f751437a58e in
JSC::Heap::runCurrentPhase(JSC::GCConductor, JSC::CurrentThreadState*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1221:18 #54 0x7f75143905fc in
JSC::Heap::collectInMutatorThread()::$_0::operator()(JSC::CurrentThreadState&) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1835:52 #55 0x7f75143905fc in
WTF::ScopedLambdaFunctor<void (JSC::CurrentThreadState&),
JSC::Heap::collectInMutatorThread()::$_0>::implFunction(void*, JSC::CurrentThreadState&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ScopedLambda.h
:106:16 #56 0x7f75143fad1d in void WTF::ScopedLambda<void
(JSC::CurrentThreadState&)>::operator()JSC::CurrentThreadState&
(JSC::CurrentThreadState&) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/ScopedLambda.h
:58:16 #57 0x7f75143fad1d in JSC::callWithCurrentThreadState(WTF::ScopedLambda<void
(JSC::CurrentThreadState&)> const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/MachineStackMarker.cpp:221:5 #58 0x7f751438638e
```

```
in JSC::Heap::collectInMutatorThread()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1847:13 #59 0x7f7514385f45 in
JSC::Heap::stopIfNecessarySlow(unsigned int)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1816:9 #60 0x7f7514385f45 in
JSC::Heap::stopIfNecessarySlow() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:1788:12 #61 0x7f751436ec6e in
JSC::Heap::stopIfNecessary() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/HeapInlines.h:270:9 #62 0x7f751436ec6e in
JSC::Heap::collectIfNecessaryOrDefer(JSC::GCDeferralContext*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/Heap.cpp:2599:13 #63 0x7f75143f8641 in
JSC::LocalAllocator::allocateSlowCase(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocator.cpp:125:10 #64 0x7f75125fdf09 in
JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode)::'lambda'()::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocatorInlines.h:40:43 #65 0x7f75125fdf09 in
JSC::HeapCell* JSC::FreeList::allocate<JSC::LocalAllocator::allocate(JSC::Heap&,
JSC::GCDeferralContext*, JSC::AllocationFailureMode)::'lambda'()>
(JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode)::'lambda'() const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/FreeListInlines.h:46:16 #66 0x7f75125fdf09 in
JSC::LocalAllocator::allocate(JSC::Heap&, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/LocalAllocatorInlines.h:37:23 #67 0x7f75125fdf09 in
JSC::Allocator::allocate(JSC::Heap&, JSC::GCDeferralContext*, JSC::AllocationFailureMode)
const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/AllocatorInlines.h:35:30 #68 0x7f75125fdf09 in
JSC::IsoSubspace::allocateNonVirtual(JSC::VM&, unsigned long, JSC::GCDeferralContext*,
JSC::AllocationFailureMode) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/heap/IsoSubspaceInlines.h:34:30 #69 0x7f75125fdf09 in
void* JSC::tryAllocateCellHelperJSC::Structure(JSC::Heap&, unsigned long,
JSC::GCDeferralContext*, JSC::AllocationFailureMode)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSCellInlines.h:180:63 #70 0x7f75125fdf09 in void*
JSC::allocateCellJSC::Structure(JSC::Heap&, unsigned long)
```

```
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSCellInlines.h:194:12 #71 0x7f75125fdf09 in
JSC::Structure::create(JSC::VM&, JSC::JSGlobalObject*, JSC::JSValue, JSC::TypeInfo const&,
JSC::ClassInfo const*, unsigned char, unsigned int)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/StructureInlines.h:63:42 #72 0x7f75155beb22 in
JSC::JSSloppyFunction::createStructure(JSC::VM&, JSC::JSGlobalObject*, JSC::JSValue)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSFunction.h:253:16 #73 0x7f75155beb22 in
JSC::JSGlobalObject::init(JSC::VM&)::$_0::operator()
(JSC::JSGlobalObject::FunctionStructures&) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSGlobalObject.cpp:745:58 #74 0x7f75155a5a6a in
JSC::JSGlobalObject::init(JSC::VM&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSGlobalObject.cpp:748:5 #75 0x7f75155d42c9 in
JSC::JSGlobalObject::finishCreation(JSC::VM&, JSC::JSObject*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/JavaScriptCore/runtime/JSGlobalObject.cpp:2590:5 #76 0x7f751c9e878e in
WebCore::JSDOMGlobalObject::finishCreation(JSC::VM&, JSC::JSObject*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMGlobalObject.cpp:255:11 #77 0x7f751ca0677f
in WebCore::JSDOMWindowBase::finishCreation(JSC::VM&, WebCore::JSWindowProxy*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSDOMWindowBase.cpp:120:11 #78 0x7f751aaabfd0
in WebCore::JSDOMWindow::finishCreation(JSC::VM&, WebCore::JSWindowProxy*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/DerivedSources/JSDOM
Window.cpp:5744:11 #79 0x7f751ca901a4 in WebCore::JSDOMWindow::create(JSC::VM&,
JSC::Structure*, WTF::Ref<WebCore::DOMWindow,
WTF::RawPtrTraitsWebCore::DOMWindow >&&, WebCore::JSWindowProxy*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/DerivedSources/JSDOM
Window.h:41:14 #80 0x7f751ca901a4 in
WebCore::JSWindowProxy::setWindow(WebCore::AbstractDOMWindow&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/JSWindowProxy.cpp:112:18 #81 0x7f751cb659a9 in
WebCore::WindowProxy::setDOMWindow(WebCore::AbstractDOMWindow*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/bindings/js/WindowProxy.cpp:173:22 #82 0x7f751e7db91b in
```

WebCore::FrameLoader::clear(WebCore::Document*, bool, bool, bool, WTF::Function<void ()>&&) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/FrameLoader.cpp:679:31 #83 0x7f751e770b00 in WebCore::DocumentWriter::begin(WTF::URL const&, bool, WebCore::Document*) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/DocumentWriter.cpp:165:23 #84 0x7f751e75b5a4 in WebCore::DocumentLoader::commitData(unsigned char const*, unsigned long) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/DocumentLoader.cpp:1221:34 #85 0x7f751a83b7eb in WebKit::WebFrameLoaderClient::committedLoad(WebCore::DocumentLoader*, unsigned char const*, int) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebKit/WebProcess/WebCoreSupport/WebFrameLoaderClient.cpp:1156:17 #86 0x7f751e76fb0c in WebCore::DocumentLoader::commitLoad(unsigned char const*, int) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/DocumentLoader.cpp:1188:27 #87 0x7f751e997bcd in WebCore::CachedRawResource::notifyClientsDataWasReceived(unsigned char const*, unsigned int) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/cache/CachedRawResource.cpp:138:12 #88 0x7f751e9972c3 in WebCore::CachedRawResource::updateBuffer(WebCore::SharedBuffer&) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/cache/CachedRawResource.cpp:75:9 #89 0x7f751e8e148f in WebCore::SubresourceLoader::didReceiveDataOrBuffer(unsigned char const*, int, WTF::RefPtr<WebCore::SharedBuffer, WTF::RawPtrTraitsWebCore::SharedBuffer, WTF::DefaultRefDerefTraitsWebCore::SharedBuffer >&&, long long, WebCore::DataPayloadType) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/SubresourceLoader.cpp:562:25 #90 0x7f751e8e1114 in WebCore::SubresourceLoader::didReceiveData(unsigned char const*, unsigned int, long long, WebCore::DataPayloadType) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebCore/loader/SubresourceLoader.cpp:530:5 #91 0x7f751a73092b in WebKit::WebResourceLoader::didReceiveData(IPC::ArrayReference<unsigned char, 18446744073709551615ul> const&, long) /root/browser/webkit/webkit_trunck_clean_version/Safari-branch/Source/WebKit/WebProcess/Network/WebResourceLoader.cpp:210:19 #92 0x7f7519591b4e in void IPC::callMemberFunctionImpl<WebKit::WebResourceLoader, void (WebKit::WebResourceLoader::*)(IPC::ArrayReference<unsigned char, 18446744073709551615ul> const&, long), std::tuple<IPC::ArrayReference<unsigned char, 18446744073709551615ul>, long>, 0ul, 1ul>(WebKit::WebResourceLoader*, void (WebKit::WebResourceLoader::*)(IPC::ArrayReference<unsigned char, 18446744073709551615ul> const&, long), std::tuple<IPC::ArrayReference<unsigned char,*

```
18446744073709551615ul>, long>&&, std::integer_sequence<unsigned long, 0ul, 1ul>)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/HandleMessage.h:125:5 #93 0x7f7519591b4e in void
IPC::callMemberFunction<WebKit::WebResourceLoader, void (WebKit::WebResourceLoader::)
(IPC::ArrayReference<unsigned char, 18446744073709551615ul> const&, long),
std::tuple<IPC::ArrayReference<unsigned char, 18446744073709551615ul>, long>,
std::integer_sequence<unsigned long, 0ul, 1ul> >(std::tuple<IPC::ArrayReference<unsigned
char, 18446744073709551615ul>, long>&&, WebKit::WebResourceLoader*, void
(WebKit::WebResourceLoader::)(IPC::ArrayReference<unsigned char,
18446744073709551615ul> const&, long))
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/HandleMessage.h:131:5 #94 0x7f7519591b4e in void
IPC::handleMessage<Messages::WebResourceLoader::DidReceiveData,
WebKit::WebResourceLoader, void (WebKit::WebResourceLoader::)
(IPC::ArrayReference<unsigned char, 18446744073709551615ul> const&, long)>
(IPC::Connection&, IPC::Decoder&, WebKit::WebResourceLoader*, void
(WebKit::WebResourceLoader::)(IPC::ArrayReference<unsigned char,
18446744073709551615ul> const&, long))
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/HandleMessage.h:202:5 #95 0x7f7519591b4e in
WebKit::WebResourceLoader::didReceiveWebResourceLoaderMessage(IPC::Connection&,
IPC::Decoder&) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/DerivedSources/WebKit/WebResourc
eLoaderMessageReceiver.cpp:54:16 #96 0x7f7519b71619 in
IPC::Connection::dispatchMessage(IPC::Decoder&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/Connection.cpp:1058:14 #97 0x7f7519b71dbe in
IPC::Connection::dispatchMessage(std::unique_ptr<IPC::Decoder,
std::default_deleteIPC::Decoder >) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/Connection.cpp:1103:9 #98 0x7f7519b729c3 in
IPC::Connection::dispatchOneIncomingMessage()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Platform/IPC/Connection.cpp:1172:5 #99 0x7f7516739dc7 in
WTF::Function<void ()>::operator()() const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/Function.h:82:35 #100 0x7f7516739dc7 in
WTF::RunLoop::performWork() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/RunLoop.cpp:133:9 #101 0x7f75168b8645 in
WTF::RunLoop::RunLoop()::$_1::operator()(void) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
```

```
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:80:42 #102 0x7f75168b8645 in
WTF::RunLoop::RunLoop()::$_1::__invoke(void*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:79:43 #103 0x7f75168b5c2c in
WTF::RunLoop::$_0::operator()(_GSource*, int ()(void), void*) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:53:28 #104 0x7f75168b5c2c in
WTF::RunLoop::$_0::__invoke(_GSource*, int ()(void), void*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:45:5 #105 0x7f750fc0304d in
g_main_context_dispatch (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x5204d) #106
0x7f750fc033ff (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x523ff) #107 0x7f750fc036f2 in
g_main_loop_run (/usr/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x526f2) #108
0x7f75168b7202 in WTF::RunLoop::run()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:108:9 #109 0x7f751a9a3c4f in
WebKit::AuxiliaryProcessMainBase<WebKit::WebProcess, true>::run(int, char**)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/AuxiliaryProcessMain.h:70:9 #110 0x7f751a9a3c4f in int
WebKit::AuxiliaryProcessMainWebKit::WebProcessMainGtk(int, char**)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/AuxiliaryProcessMain.h:96:27 #111 0x7f751a9a3c4f in
WebKit::WebProcessMain(int, char**)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/WebProcess/gtk/WebProcessMainGtk.cpp:87:12 #112
0x7f750f59f0b2 in __libc_start_main (/lib/x86_64-linux-gnu/libc.so.6+0x270b2) #113
0x41d37d in _start (/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/bin/WebKitWebProcess+0x41d37d)
```

```
0x61b00012d7b8 is located 56 bytes inside of 1488-byte region
[0x61b00012d780,0x61b00012dd50) freed by thread T44 (eadedCompositor) here: #0
0x4c2bd7 in free /root/llvm/llvm-12/compiler-rt/lib/asan/asan_malloc_linux.cpp:127:3 #1
0x7f7519cdf8ea in WebKit::CoordinatedGraphicsScene::updateSceneState()::$_0::operator()
(Nicosia::Scene::State&) const /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/CoordinatedGraphicsScene.cpp:264:1
7 #2 0x7f7519cdf8ea in void
Nicosia::Scene::accessStateWebKit::CoordinatedGraphicsScene::updateSceneState()::$_0(We
bKit::CoordinatedGraphicsScene::updateSceneState()::$_0 const&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WebCore/PrivateHeaders/WebCore
/NicosiaScene.h:66:9 #3 0x7f7519cdf8ea in
WebKit::CoordinatedGraphicsScene::updateSceneState()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/CoordinatedGraphicsScene.cpp:235:2
2 #4 0x7f7519cde311 in
WebKit::CoordinatedGraphicsScene::paintToCurrentGLContext(WebCore::TransformationMa
trix const&, WebCore::FloatRect const&, unsigned int)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/CoordinatedGraphicsScene.cpp:65:5
#5 0x7f7519cef1e8 in WebKit::ThreadedCompositor::renderLayerTree()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/ThreadedComp
ositor.cpp:235:14 #6 0x7f75168b8774 in
WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::operator()(void*) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:177:16 #7 0x7f75168b8774 in
WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::__invoke(void*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:169:43
```

```
previously allocated by thread T44 (eadedCompositor) here: #0 0x4c2ecf in malloc
/root/llvm/llvm-12/compiler-rt/lib/asan/asan_malloc_linux.cpp:145:3 #1 0x7f75168cc72a in
bmalloc::DebugHeap::malloc(unsigned long, bmalloc::FailureAction)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/bmalloc/bmalloc/DebugHeap.cpp:102:20 #2 0x7f7519cde311 in
WebKit::CoordinatedGraphicsScene::paintToCurrentGLContext(WebCore::TransformationMa
trix const&, WebCore::FloatRect const&, unsigned int)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/CoordinatedGraphicsScene.cpp:65:5
#3 0x7f7519cef1e8 in WebKit::ThreadedCompositor::renderLayerTree()
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/ThreadedComp
ositor.cpp:235:14 #4 0x7f75168b8774 in
WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::operator()(void*) const
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:177:16 #5 0x7f75168b8774 in
WTF::RunLoop::TimerBase::TimerBase(WTF::RunLoop&)::$_3::__invoke(void*)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/glib/RunLoopGLib.cpp:169:43
```

```
Thread T44 (eadedCompositor) created by T0 here: #0 0x4348a6 in pthread_create
/root/llvm/llvm-12/compiler-rt/lib/asan/asan_interceptors.cpp:205:3 #1 0x7f75168c0658 in
WTF::Thread::establishHandle(WTF::Thread::NewThreadContext*, std::optional,
WTF::Thread::QOS) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/posix/ThreadingPOSIX.cpp:275:17 #2 0x7f7516744b25 in
WTF::Thread::create(char const*, WTF::Function<void ()>&&, WTF::ThreadType,
WTF::Thread::QOS) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WTF/wtf/Threading.cpp:203:32 #3 0x7f7519ce966f in
WebKit::createRunLoop() /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/CompositingRu
nLoop.cpp:46:5 #4 0x7f7519ce966f in
WebKit::CompositingRunLoop::CompositingRunLoop(WTF::Function<void ()>&&)
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/CompositingRu
nLoop.cpp:57:17 #5 0x7f7519ceb0af in
std::_MakeUniqWebKit::CompositingRunLoop::__single_object
std::make_unique<WebKit::CompositingRunLoop,
WebKit::ThreadedCompositor::ThreadedCompositor(WebKit::ThreadedCompositor::Client&,
WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int)::$_6>
(WebKit::ThreadedCompositor::ThreadedCompositor(WebKit::ThreadedCompositor::Client&
, WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int)::$_6&&) /usr/lib/gcc/x86_64-linux-
gnu/9/../../../../include/c++/9/bits/unique_ptr.h:857:34 #6 0x7f7519ceb0af in decltype(auto)
WTF::makeUnique<WebKit::CompositingRunLoop,
WebKit::ThreadedCompositor::ThreadedCompositor(WebKit::ThreadedCompositor::Client&,
WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int)::$_6>
(WebKit::ThreadedCompositor::ThreadedCompositor(WebKit::ThreadedCompositor::Client&
, WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int)::$_6&&) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/WebKitBuild_Asan_RelWithDebug/GTK/Release/WTF/Headers/wtf/StdLibExtras.h:50
9:12 #7 0x7f7519ceb0af in
WebKit::ThreadedCompositor::ThreadedCompositor(WebKit::ThreadedCompositor::Client&,
WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/ThreadedComp
ositor.cpp:58:28 #8 0x7f7519ceae4e in
WebKit::ThreadedCompositor::create(WebKit::ThreadedCompositor::Client&,
WebKit::ThreadedDisplayRefreshMonitor::Client&, unsigned int, WebCore::IntSize const&,
float, unsigned int) /root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebKit/Shared/CoordinatedGraphics/threadedcompositor/ThreadedComp
ositor.cpp:52:26
```

```
SUMMARY: AddressSanitizer: heap-use-after-free
/root/browser/webkit/webkit_trunck_clean_version/Safari-
branch/Source/WebCore/platform/graphics/texmap/TextureMapperLayer.cpp:702:21 in
WebCore::TextureMapperLayer::setContentsLayer(WebCore::TextureMapperPlatformLayer*)
Shadow bytes around the buggy address: 0x0c368001daa0: fd fd fd fd fd fd fd fd fd fd fd fd
fd fd fd fd 0x0c368001dab0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0x0c368001dac0: fd
fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa 0x0c368001dad0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa
fa fa 0x0c368001dae0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa =>0x0c368001daf0: fd fd fd
fd fd fd fd[fd]fd fd fd fd fd fd fd fd 0x0c368001db00: fd fd fd fd fd fd fd fd fd fd fd fd fd
fd fd 0x0c368001db10: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0x0c368001db20: fd fd
fd fd fd fd fd fd fd fd fd fd fd fd fd fd 0x0c368001db30: fd fd fd fd fd fd fd fd fd fd fd fd
fd fd fd 0x0c368001db40: 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 ==18385==ABORTING
```