Starred by 5 users

Owner:	dhoss@chromium.org **Last visit 17 days ago**
CC:	a...@microsoft.com rsesek@chromium.org thestig@chromium.org kmoon@chromium.org
Status:	Verified *(Closed)*
Components:	Internals>Plugins>PDF>Accessibility
Modified:	Oct 5, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-97
external_security_report
M-96
FoundIn-96
Security_Impact-Extended
merge-merged-4692
merge-merged-97
Release-0-M97
CVE-2022-0105
Team-Accessibility

Issue 1274376: uaf in chrome_pdf::PdfViewPluginBase::LoadAccessibility

Reported by emily...@gmail.com on Sun, Nov 28, 2021, 12:32 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36

Steps to reproduce the problem:
Ubunt 20.04

Chrome version
Version Chromium 98.0.4710.4 (Developer Build) (64-bit) with asan build
Chromium 98.0.4733.0 (Developer Build) (64-bit) gs://chromium-browser-asan/linux-release/asan-linux-release-945734.zip

1 ./chrome -force-renderer-accessibility --user-data-dir=/tmp/xx http://localhost:8000/crash.html
2 The print dialog box and the "pop-up-blocked" prompt box will pop up.
3.Click "alwayse allow pop--up" and then click refresh again.
The repro is not very stable in the local test, and it can be reproduced about once every 10 times.
During the test, there will be many CHECK crashes of the browser process,and just restart the browser again.

What is the expected behavior?

What went wrong?
==1==ERROR: AddressSanitizer: heap-use-after-free on address 0x61a00000a898 at pc 0x560c9a3525d1 bp 0x7fff894f91b0 sp 0x7fff894f91a8
READ of size 8 at 0x61a00000a898 thread T0 (chrome)
    #0 0x560c9a3525d0 in chrome_pdf::PdfViewPluginBase::LoadAccessibility() ./../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:284
    #1 0x560c9a3525d0 in LoadAccessibility ./../../pdf/pdf_view_plugin_base.cc:1635
    #2 0x560c9a3525d0 in ?? ??:0
    #3 0x560c9a3564a2 in chrome_pdf::PdfViewPluginBase::DocumentLoadComplete() ./../../pdf/pdf_view_plugin_base.cc:436
    #4 0x560c9a3564a2 in ?? ??:0
    #5 0x560c9a370fe2 in chrome_pdf::PDFiumEngine::FinishLoadingDocument(int) ./../../pdf/pdfium/pdfium_engine.cc:898
    #6 0x560c9a370fe2 in ?? ??:0
    #7 0x560c9a397b7d in chrome_pdf::PDFiumEngine::ContinueLoadingDocument(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&) ./../../pdf/pdfium/pdfium_engine.cc:2795
    #8 0x560c9a397b7d in ?? ??:0
    #9 0x560c9a375ca1 in chrome_pdf::PDFiumEngine::LoadDocument() ./../../pdf/pdfium/pdfium_engine.cc:2718
    #10 0x560c9a375ca1 in ?? ??:0
    #11 0x560c9a33ff51 in chrome_pdf::DocumentLoaderImpl::DidRead(int) document_loader_impl.cc:?
    #12 0x560c9a33ff51 in ?? ??:0
    #13 0x560c9a340d75 in base::internal::Invoker<base::internal::BindState<void (chrome_pdf::DocumentLoaderImpl::*)(int), base::WeakPtr<chrome_pdf::DocumentLoaderImpl> >, void (int)>::RunOnce(base::internal::BindStateBase*, int) ./../../base/bind_internal.h:533
    #14 0x560c9a340d75 in MakeItSo<void (chrome_pdf::DocumentLoaderImpl::*)(int), base::WeakPtr<chrome_pdf::DocumentLoaderImpl>, int> ./../../base/bind_internal.h:728

    #15 0x560c9a340d75 in RunImpl<void (chrome_pdf::DocumentLoaderImpl::*)(int), std::__1::tuple<base::WeakPtr<chrome_pdf::DocumentLoaderImpl> >, 0UL> ./../../base/bind_internal.h:781
    #16 0x560c9a340d75 in RunOnce ./../../base/bind_internal.h:750

#16 0x560c9a340d75 in RunOnce ./../../base/bind_internal.h:750
#17 0x560c9a340d75 in ?? ??:0
#18 0x560c9a3e74a5 in chrome_pdf::URLLoaderWrapperImpl::DidRead(base::OnceCallback<void (int)>, int) ./../../base/callback.h:142
#19 0x560c9a3e74a5 in DidRead ./../../pdf/url_loader_wrapper_impl.cc:248
#20 0x560c9a3e74a5 in ?? ??:0
#21 0x560c9a3f07e6 in base::internal::Invoker<base::internal::BindState<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>, int), base::WeakPtr<chrome_pdf::URLLoaderWrapperImpl>, base::OnceCallback<void (int)> >, void (int)>::RunOnce(base::internal::BindStateBase*, int) ./../../base/bind_internal.h:533
#22 0x560c9a3f07e6 in MakeItSo<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>, int), base::WeakPtr<chrome_pdf::URLLoaderWrapperImpl>, base::OnceCallback<void (int)>, int> ./../../base/bind_internal.h:728
#23 0x560c9a3f07e6 in RunImpl<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>, int), std::__1::tuple<base::WeakPtr<chrome_pdf::URLLoaderWrapperImpl>, base::OnceCallback<void (int)> >, 0UL, 1UL> ./../../base/bind_internal.h:781
#24 0x560c9a3f07e6 in RunOnce ./../../base/bind_internal.h:750
#25 0x560c9a3f07e6 in ?? ??:0
#26 0x560c9a3fb494 in chrome_pdf::BlinkUrlLoader::RunReadCallback() ./../../base/callback.h:142
#27 0x560c9a3fb494 in RunReadCallback ./../../pdf/ppapi_migration/url_loader.cc:318
#28 0x560c9a3fb494 in ?? ??:0
#29 0x560c9a3fae8b in chrome_pdf::BlinkUrlLoader::ReadResponseBody(base::span<char, 18446744073709551615ul>, base::OnceCallback<void (int)>) ./../../pdf/ppapi_migration/url_loader.cc:179
#30 0x560c9a3fae8b in ?? ??:0
#31 0x560c9a3e7130 in chrome_pdf::URLLoaderWrapperImpl::ReadResponseBodyImpl(base::OnceCallback<void (int)>) ./../../pdf/url_loader_wrapper_impl.cc:176
#32 0x560c9a3e7130 in ?? ??:0
#33 0x560c9a3f0aaa in base::internal::Invoker<base::internal::BindState<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>), base::internal::UnretainedWrapper<chrome_pdf::URLLoaderWrapperImpl>, base::OnceCallback<void (int)> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:533
#34 0x560c9a3f0aaa in MakeItSo<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>), chrome_pdf::URLLoaderWrapperImpl *, base::OnceCallback<void (int)> > ./../../base/bind_internal.h:708
#35 0x560c9a3f0aaa in RunImpl<void (chrome_pdf::URLLoaderWrapperImpl::*)(base::OnceCallback<void (int)>), std::__1::tuple<base::internal::UnretainedWrapper<chrome_pdf::URLLoaderWrapperImpl>, base::OnceCallback<void (int)> >, 0UL, 1UL> ./../../base/bind_internal.h:781
#36 0x560c9a3f0aaa in RunOnce ./../../base/bind_internal.h:750
#37 0x560c9a3f0aaa in ?? ??:0
#38 0x560c9c6239b0 in base::OneShotTimer::RunUserTask() ./../../base/callback.h:142
#39 0x560c9c6239b0 in RunUserTask ./../../base/timer/timer.cc:290
#40 0x560c9c6239b0 in ?? ??:0
#41 0x560c9c5c9132 in base::DefaultDelayedTaskHandleDelegate::RunTask(base::OnceCallback<void ()>) ./../../base/callback.h:142
#42 0x560c9c5c9132 in RunTask ./../../base/task/default_delayed_task_handle_delegate.cc:36
#43 0x560c9c5c9132 in ?? ??:0
#44 0x560c9c5c942f in base::internal::Invoker<base::internal::BindState<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>), base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, void ()>::RunOnce(base::internal::BindStateBase*) ./../../base/bind_internal.h:533
#45 0x560c9c5c942f in MakeItSo<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>), base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> > ./../../base/bind_internal.h:728
#46 0x560c9c5c942f in RunImpl<void (base::DefaultDelayedTaskHandleDelegate::*)(base::OnceCallback<void ()>), std::__1::tuple<base::WeakPtr<base::DefaultDelayedTaskHandleDelegate>, base::OnceCallback<void ()> >, 0UL, 1UL> ./../../base/bind_internal.h:781

#47 0x560c9c5c942f in RunOnce ./../../base/bind_internal.h:750
#48 0x560c9c5c942f in ?? ??:0
#49 0x560c9c5827e3 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) ./../../base/callback.h:142

#49 0x560c9c5827e3 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) ./../../base/callback.h:142
#50 0x560c9c5827e3 in RunTaskImpl ./../../base/task/common/task_annotator.cc:135
#51 0x560c9c5827e3 in ?? ??:0
#52 0x560c9c5bcf23 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) ./../../base/task/common/task_annotator.h:73
#53 0x560c9c5bcf23 in DoWorkImpl
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356
#54 0x560c9c5bcf23 in ?? ??:0
#55 0x560c9c5bc737 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261
#56 0x560c9c5bc737 in ?? ??:0
#57 0x560c9c5bdaf1 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:?
#58 0x560c9c5bdaf1 in ?? ??:0
#59 0x560c9c47782f in base::MessagePumpDefault::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_default.cc:38
#60 0x560c9c47782f in ?? ??:0
#61 0x560c9c5be1bb in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468
#62 0x560c9c5be1bb in ?? ??:0
#63 0x560c9c4fabc9 in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:140
#64 0x560c9c4fabc9 in ?? ??:0
#65 0x560cb080e11d in content::RendererMain(content::MainFunctionParams)
./../../content/renderer/renderer_main.cc:267
#66 0x560cb080e11d in ?? ??:0
#67 0x560c9b34f110 in content::RunZygote(content::ContentMainDelegate*)
./../../content/app/content_main_runner_impl.cc:615
#68 0x560c9b34f110 in ?? ??:0
#69 0x560c9b351c6e in content::RunOtherNamedProcessTypeMain(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, content::MainFunctionParams,
content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:687
#70 0x560c9b351c6e in ?? ??:0
#71 0x560c9b353af7 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1028
#72 0x560c9b353af7 in ?? ??:0
#73 0x560c9b34c63c in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:398
#74 0x560c9b34c63c in ?? ??:0
#75 0x560c9b34e264 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:426
#76 0x560c9b34e264 in ?? ??:0
#77 0x560c8e35c9de in ChromeMain ./../../chrome/app/chrome_main.cc:172
#78 0x560c8e35c9de in ?? ??:0
#79 0x7fc1c0f210b2 in __libc_start_main ??:?
#80 0x7fc1c0f210b2 in ?? ??:0

0x61a00000a898 is located 24 bytes inside of 1272-byte region [0x61a00000a880,0x61a00000ad78)
freed by thread T0 (chrome) here:
#0 0x560c8e35a99d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:152
#1 0x560c8e35a99d in ?? ??:0

#2 0x560caccd4009 in blink::WebPluginContainerImpl::Dispose()
./../../third_party/blink/renderer/core/exported/web_plugin_container_impl.cc:796
#3 0x560caccd4009 in ?? ??:0

#3 0x560cacca4009 in ?? ??:0
#4 0x560ca9c4afc6 in blink::HTMLFrameOwnerElement::PluginDisposeSuspendScope::PerformDeferredPluginDispose()
./../../third_party/blink/renderer/core/html/html_frame_owner_element.cc:265
#5 0x560ca9c4afc6 in ?? ??:0
#6 0x560ca9c9dd8e in blink::HTMLPlugInElement::AttachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/html/html_frame_owner_element.h:88
#7 0x560ca9c9dd8e in AttachLayoutTree ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:208
#8 0x560ca9c9dd8e in ?? ??:0
#9 0x560ca8a6fa46 in blink::ContainerNode::AttachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/dom/container_node.cc:1054
#10 0x560ca8a6fa46 in ?? ??:0
#11 0x560ca8a04bdd in blink::Element::AttachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/dom/element.cc:2761
#12 0x560ca8a04bdd in ?? ??:0
#13 0x560ca8a6fa46 in blink::ContainerNode::AttachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/dom/container_node.cc:1054
#14 0x560ca8a6fa46 in ?? ??:0
#15 0x560ca8a04bdd in blink::Element::AttachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/dom/element.cc:2761
#16 0x560ca8a04bdd in ?? ??:0
#17 0x560ca89a95da in blink::Node::ReattachLayoutTree(blink::Node::AttachContext&)
./../../third_party/blink/renderer/core/dom/node.cc:1546
#18 0x560ca89a95da in ?? ??:0
#19 0x560ca8a13e59 in blink::Element::RebuildLayoutTree(blink::WhitespaceAttacher&)
./../../third_party/blink/renderer/core/dom/element.cc:3393
#20 0x560ca8a13e59 in ?? ??:0
#21 0x560ca8ac120f in blink::StyleEngine::RebuildLayoutTree()
./../../third_party/blink/renderer/core/css/style_engine.cc:2360
#22 0x560ca8ac120f in ?? ??:0
#23 0x560ca8ac2a9f in blink::StyleEngine::UpdateStyleAndLayoutTree()
./../../third_party/blink/renderer/core/css/style_engine.cc:2406
#24 0x560ca8ac2a9f in ?? ??:0
#25 0x560ca884c877 in blink::Document::UpdateStyle() ./../../third_party/blink/renderer/core/dom/document.cc:2185
#26 0x560ca884c877 in ?? ??:0
#27 0x560ca884b04f in blink::Document::UpdateStyleAndLayoutTreeForThisDocument()
./../../third_party/blink/renderer/core/dom/document.cc:2134
#28 0x560ca884b04f in ?? ??:0
#29 0x560ca909cac8 in blink::LocalFrameView::UpdateStyleAndLayoutInternal()
./../../third_party/blink/renderer/core/frame/local_frame_view.cc:3376
#30 0x560ca909cac8 in ?? ??:0
#31 0x560ca9082a65 in blink::LocalFrameView::UpdateStyleAndLayout()
./../../third_party/blink/renderer/core/frame/local_frame_view.cc:3330
#32 0x560ca9082a65 in ?? ??:0
#33 0x560ca9091868 in blink::LocalFrameView::UpdateStyleAndLayoutIfNeededRecursive()
./../../third_party/blink/renderer/core/frame/local_frame_view.cc:3250
#34 0x560ca9091868 in ?? ??:0
#35 0x560ca908dc3c in
blink::LocalFrameView::RunStyleAndLayoutLifecyclePhases(blink::DocumentLifecycle::LifecycleState)
./../../third_party/blink/renderer/core/frame/local_frame_view.cc:2604
#36 0x560ca908dc3c in ?? ??:0
#37 0x560ca908c99b in blink::LocalFrameView::UpdateLifecyclePhasesInternal(blink::DocumentLifecycle::LifecycleState)

./../../third_party/blink/renderer/core/frame/local_frame_view.cc:2425
#38 0x560ca908c99b in ?? ??:0
#39 0x560ca908a1fa in blink::LocalFrameView::UpdateLifecyclePhases(blink::DocumentLifecycle::LifecycleState

#39 0x560ca908a1fc in blink::LocalFrameView::UpdateLifecyclePhases(blink::DocumentLifecycle::LifecycleState, blink::DocumentUpdateReason) ./../../third_party/blink/renderer/core/frame/local_frame_view.cc:2366
#40 0x560ca908a1fc in ?? ??:0
#41 0x560cacd5e343 in blink::WebAXObject::MaybeUpdateLayoutAndCheckValidity(blink::WebDocument const&) ./../../third_party/blink/renderer/modules/exported/web_ax_object.cc:1398
#42 0x560cacd5e343 in ?? ??:0
#43 0x560cacd68df7 in blink::WebAXObject::FromWebDocument(blink::WebDocument const&) ./../../third_party/blink/renderer/modules/exported/web_ax_object.cc:1344
#44 0x560cacd68df7 in ?? ??:0
#45 0x560cad31bc28 in content::BlinkAXTreeSource::ComputeRoot() const ./../../content/renderer/accessibility/blink_ax_tree_source.cc:614
#46 0x560cad31bc28 in ?? ??:0
#47 0x560cad31fa15 in content::BlinkAXTreeSource::GetRoot() const ./../../content/renderer/accessibility/blink_ax_tree_source.cc:383
#48 0x560cad31fa15 in ?? ??:0
#49 0x560cad305340 in content::RenderAccessibilityImpl::GenerateAXID() ./../../content/renderer/accessibility/render_accessibility_impl.cc:728
#50 0x560cad305340 in ?? ??:0
#51 0x560cb0aebec7 in pdf::PdfAccessibilityTree::GetRenderAccessibilityIfEnabled() ./../../components/pdf/renderer/pdf_accessibility_tree.cc:1515
#52 0x560cb0aebec7 in ?? ??:0
#53 0x560cb0aec30d in pdf::PdfAccessibilityTree::SetAccessibilityDocInfo(chrome_pdf::AccessibilityDocInfo const&) ./../../components/pdf/renderer/pdf_accessibility_tree.cc:1323
#54 0x560cb0aec30d in ?? ??:0
#55 0x560c9a351f85 in chrome_pdf::PdfViewPluginBase::LoadAccessibility() ./../../pdf/pdf_view_plugin_base.cc:1632
#56 0x560c9a351f85 in ?? ??:0
#57 0x560c9a3564a2 in chrome_pdf::PdfViewPluginBase::DocumentLoadComplete() ./../../pdf/pdf_view_plugin_base.cc:436
#58 0x560c9a3564a2 in ?? ??:0
#59 0x560c9a370fe2 in chrome_pdf::PDFiumEngine::FinishLoadingDocument(int) ./../../pdf/pdfium/pdfium_engine.cc:898
#60 0x560c9a370fe2 in ?? ??:0

previously allocated by thread T0 (chrome) here:
#0 0x560c8e35a13d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:95
#1 0x560c8e35a13d in ?? ??:0
#2 0x560cb0ad41bd in pdf::CreateInternalPlugin(content::WebPluginInfo const&, blink::WebPluginParams, content::RenderFrame*, std::__1::unique_ptr<pdf::PdfInternalPluginDelegate, std::__1::default_delete<pdf::PdfInternalPluginDelegate> >) ./../../components/pdf/renderer/internal_plugin_renderer_helpers.cc:70
#3 0x560cb0ad41bd in ?? ??:0
#4 0x560cad0d96b2 in ChromeContentRendererClient::CreatePlugin(content::RenderFrame*, blink::WebPluginParams const&, chrome::mojom::PluginInfo const&) ./../../chrome/renderer/chrome_content_renderer_client.cc:1084
#5 0x560cad0d96b2 in ?? ??:0
#6 0x560cad0d62f7 in ChromeContentRendererClient::OverrideCreatePlugin(content::RenderFrame*, blink::WebPluginParams const&, blink::WebPlugin**) ./../../chrome/renderer/chrome_content_renderer_client.cc:837
#7 0x560cad0d62f7 in ?? ??:0
#8 0x560cad29a1e2 in content::RenderFrameImpl::CreatePlugin(blink::WebPluginParams const&) ./../../content/renderer/render_frame_impl.cc:3335
#9 0x560cad29a1e2 in ?? ??:0
#10 0x560ca99682b9 in blink::LocalFrameClientImpl::CreatePlugin(blink::HTMLPlugInElement&, blink::KURL const&,

WTF::Vector<WTF::String, 0u, WTF::PartitionAllocator> const&, WTF::Vector<WTF::String, 0u, WTF::PartitionAllocator> const&, WTF::String const&, bool) ./../../third_party/blink/renderer/core/frame/local_frame_client_impl.cc:891
#11 0x560ca99682b9 in ?? ??:0

#11 0x560ca99682b9 in ?? ??:0
#12 0x560ca9ca3ed8 in blink::HTMLPlugInElement::LoadPlugin(blink::KURL const&, WTF::String const&, blink::PluginParameters const&, bool) ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:678
#13 0x560ca9ca3ed8 in ?? ??:0
#14 0x560ca9ca2514 in blink::HTMLPlugInElement::RequestObject(blink::PluginParameters const&) ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:648
#15 0x560ca9ca2514 in ?? ??:0
#16 0x560ca9c442ad in blink::HTMLEmbedElement::UpdatePluginInternal() ./../../third_party/blink/renderer/core/html/html_embed_element.cc:178
#17 0x560ca9c442ad in ?? ??:0
#18 0x560ca9c9efdd in blink::HTMLPlugInElement::UpdatePlugin() ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:262
#19 0x560ca9c9efdd in ?? ??:0
#20 0x560ca9087283 in blink::LocalFrameView::UpdatePlugins() ./../../third_party/blink/renderer/core/frame/local_frame_view.cc:1866
#21 0x560ca9087283 in ?? ??:0
#22 0x560ca908759c in blink::LocalFrameView::FlushAnyPendingPostLayoutTasks() ./../../third_party/blink/renderer/core/frame/local_frame_view.cc:1881
#23 0x560ca908759c in FlushAnyPendingPostLayoutTasks ./../../third_party/blink/renderer/core/frame/local_frame_view.cc:1890
#24 0x560ca908759c in ?? ??:0
#25 0x560ca9ca1141 in blink::HTMLPlugInElement::LayoutEmbeddedContentForJSBindings() const ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:488
#26 0x560ca9ca1141 in ?? ??:0
#27 0x560ca9ca05c3 in blink::HTMLPlugInElement::PluginWrapper() ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:412
#28 0x560ca9ca05c3 in PluginWrapper ./../../third_party/blink/renderer/core/html/html_plugin_element.cc:390
#29 0x560ca9ca05c3 in ?? ??:0
#30 0x560cac58017b in blink::V8HTMLEmbedElement::NamedPropertyGetterCustom(WTF::AtomicString const&, v8::PropertyCallbackInfo<v8::Value> const&) ./../../third_party/blink/renderer/bindings/core/v8/custom/v8_html_plugin_element_custom.cc:67
#31 0x560cac58017b in NamedPropertyGetterCustom ./../../third_party/blink/renderer/bindings/core/v8/custom/v8_html_plugin_element_custom.cc:138
#32 0x560cac58017b in ?? ??:0
#33 0x560cac57a134 in blink::V8HTMLEmbedElement::NamedPropertyGetterCallback(v8::Local<v8::Name>, v8::PropertyCallbackInfo<v8::Value> const&) ./gen/third_party/blink/renderer/bindings/core/v8/v8_html_embed_element.cc:85
#34 0x560cac57a134 in ?? ??:0
#35 0x560c9727c27e in v8::internal::PropertyCallbackArguments::CallNamedGetter(v8::internal::Handle<v8::internal::InterceptorInfo>, v8::internal::Handle<v8::internal::Name>) ./../../v8/src/api/api-arguments-inl.h:204
#36 0x560c9727c27e in CallNamedGetter ./../../v8/src/api/api-arguments-inl.h:181
#37 0x560c9727c27e in ?? ??:0
#38 0x560c97738c81 in v8::internal::(anonymous namespace)::GetPropertyWithInterceptorInternal(v8::internal::LookupIterator*, v8::internal::Handle<v8::internal::InterceptorInfo>, bool*) ./../../v8/src/objects/js-objects.cc:1140
#39 0x560c97738c81 in ?? ??:0
#40 0x560c97825a91 in v8::internal::Object::GetProperty(v8::internal::LookupIterator*, bool) ./../../v8/src/objects/objects.cc:1159
#41 0x560c97825a91 in ?? ??:0
#42 0x560c97231f21 in v8::internal::LoadIC::Load(v8::internal::Handle<v8::internal::Object>,

v8::internal::Handle<v8::internal::Name>, bool, v8::internal::Handle<v8::internal::Object>) ./../../v8/src/ic/ic.cc:498
#43 0x560c97231f21 in ?? ??:0
#44 0x560c97253c68 in v8::internal::Runtime_LoadNoFeedbackIC_Miss(int, unsigned long*, v8::internal::Isolate*)

```
    #44 0x560c97253c68 in v8::internal::Runtime_LoadNoFeedbackIC_Miss(int, unsigned long*, v8::internal::Isolate*)
./../../v8/src/ic/ic.cc:2596
    #45 0x560c97253c68 in Runtime_LoadNoFeedbackIC_Miss ./../../v8/src/ic/ic.cc:2581
    #46 0x560c97253c68 in ?? ??:0
    #47 0x560c98f877b7 in Builtins_CEntry_Return1_DontSaveFPRegs_ArgvOnStack_NoBuiltinExit setup-isolate-
deserialize.cc:?
    #48 0x560c98f877b7 in ?? ??:0
    #49 0x560c9901d444 in Builtins_LdaNamedPropertyHandler setup-isolate-deserialize.cc:?
    #50 0x560c9901d444 in ?? ??:0
    #51 0x560c98f0b061 in Builtins_InterpreterEntryTrampoline setup-isolate-deserialize.cc:?
    #52 0x560c98f0b061 in ?? ??:0
    #53 0x560c98f44291 in Builtins_GeneratorPrototypeNext setup-isolate-deserialize.cc:?
    #54 0x560c98f44291 in ?? ??:0
    #55 0x560c98f0905b in Builtins_JSEntryTrampoline setup-isolate-deserialize.cc:?
    #56 0x560c98f0905b in ?? ??:0
    #57 0x560c98f08d86 in Builtins_JSEntry setup-isolate-deserialize.cc:?
    #58 0x560c98f08d86 in ?? ??:0
    #59 0x560c96e94dc6 in v8::internal::(anonymous namespace)::Invoke(v8::internal::Isolate*, v8::internal::(anonymous
namespace)::InvokeParams const&) ./../../v8/src/execution/simulator.h:152
    #60 0x560c96e94dc6 in Invoke ./../../v8/src/execution/execution.cc:419
    #61 0x560c96e94dc6 in ?? ??:0
    #62 0x560c96e9907a in v8::internal::(anonymous namespace)::InvokeWithTryCatch(v8::internal::Isolate*, v8::internal::
(anonymous namespace)::InvokeParams const&) ./../../v8/src/execution/execution.cc:480
    #63 0x560c96e9907a in ?? ??:0
    #64 0x560c96e99648 in v8::internal::Execution::TryCall(v8::internal::Isolate*, v8::internal::Handle<v8::internal::Object>,
v8::internal::Handle<v8::internal::Object>, int, v8::internal::Handle<v8::internal::Object>*,
v8::internal::Execution::MessageHandling, v8::internal::MaybeHandle<v8::internal::Object>*, bool)
./../../v8/src/execution/execution.cc:580
    #65 0x560c96e99648 in ?? ??:0

SUMMARY: AddressSanitizer: heap-use-after-free (/home/exp11/asan-linux-release/chrome+0x169145d0)
Shadow bytes around the buggy address:
  0x0c347fff94c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff94d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff94e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c347fff94f0: 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c347fff9500: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c347fff9510: fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c347fff9520: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c347fff9530: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c347fff9540: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c347fff9550: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c347fff9560: 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 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
==1==ABORTING
```

Did this work before? N/A

Chrome version: 98.0.4710.4 Channel: dev
OS Version: 20.04

crash.html
2.2 KB View Download

Comment 1 by sheriffbot on Sun, Nov 28, 2021, 12:42 PM EST Project Member

Labels: external_security_report

Comment 2 by rsesek@chromium.org on Mon, Nov 29, 2021, 5:10 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: dhoss@chromium.org
Cc: thestig@chromium.org
Labels: Security_Severity-High FoundIn-96 Pri-1
Components: Internals>Plugins>PDF>Accessibility

I can't reproduce this, but the reporter does note that this is not totally reliable.

Comment 3 by thestig@chromium.org on Mon, Nov 29, 2021, 5:18 PM EST Project Member

From a previous bug from the same bug reporter, I had to adjust the code to reproduce the issue more reliably.
https://bugs.chromium.org/p/chromium/issues/detail?id=1255332#c6

Comment 4 by sheriffbot on Mon, Nov 29, 2021, 5:18 PM EST Project Member

Labels: Security_Impact-Extended

Comment 5 by thestig@chromium.org on Mon, Nov 29, 2021, 6:48 PM EST Project Member

Cc: rsesek@chromium.org

rsesek@: Did you mean to set FoundIn-98 instead?

Comment 6 by rsesek@chromium.org on Mon, Nov 29, 2021, 6:51 PM EST Project Member

The relevant code appears the same between M96 and M98:
https://source.chromium.org/chromium/chromium/src/+/refs/tags/96.0.4664.55:pdf/pdf_view_plugin_base.cc;drc=5b3bfa294c4d7b314a075ab7f8b53c7ede141fc2

But if this only happens on M98 then feel free to adjust the lables.

Comment 7 by dhoss@chromium.org on Mon, Nov 29, 2021, 6:56 PM EST Project Member

From the call-stack, it appears that this UaF is occurring on the Unseasoned PDF viewer (with chrome://flags/#pdf-unseasoned enabled).

I'll try to verify, but if it's only occurring on the Unseasoned viewer, it shouldn't be affecting any stable users.

Comment 8 by thestig@chromium.org on Mon, Nov 29, 2021, 7:00 PM EST Project Member

Cc: kmoon@chromium.org a...@microsoft.com

+kmoon@ and ankk@ FYI. This may be specific to the PPAPI-free PDF Viewer. I think SetAccessibilityDocInfo() is synchronous there, whereas in the PPAPI version, SetAccessibilityDocInfo() is asynchronous.

Yes, the code has been around since M96. Though it is controlled by a field trial and shouldn't be generally available to users on Stable Channel.

Comment 9 by sheriffbot on Tue, Nov 30, 2021, 12:46 PM EST Project Member

Labels: Target-96 M-96

Setting milestone and target because of high severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 10 by kmoon@chromium.org on Wed, Dec 1, 2021, 11:20 AM EST Project Member

We're not planning to go to Stable on M96. We are planning to go to Stable on M97, so we should backport a fix to M97 at least.

Comment 11 by thestig@chromium.org on Wed, Dec 1, 2021, 1:19 PM EST Project Member

Labels: -M-96 -Target-96 Target-97

We probably just need to add another WeakPtr to watch for self-deletion. If we are going to backport to M97, let's get this in before the M97 Stable cut.

Comment 12 by dhoss@chromium.org on Wed, Dec 1, 2021, 1:28 PM EST Project Member

Yup. Just to give an update, I've moved this up my personal priority queue.

Comment 13 by sheriffbot on Thu, Dec 2, 2021, 12:47 PM EST Project Member

Labels: -Target-97 Target-96 M-96

Setting milestone and target because of high severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 14 by Git Watcher on Fri, Dec 3, 2021, 2:39 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6d9638366ae0f60f8d2db41857fcbc738c2514d4

commit 6d9638366ae0f60f8d2db41857fcbc738c2514d4
Author: Daniel Hosseinian <dhoss@chromium.org>
Date: Fri Dec 03 19:38:47 2021

[unseasoned-pdf] Call PdfViewWebPlugin a11y methods asynchr

[unseasoned-pdf] Call PdfViewWebPlugin a11y methods asyncly

Calling a11y methods asyncly protects against the self-deletions they
may cause. The a11y methods call
content::RenderAccessibility::GenerateAXID() underneath, which may
cause a relayout which causes the PdfViewWebPlugin to be deleted.

Isolating the calls in posted tasks is a clean way to protect against
continuing control flow in the object after it is deleted.

~~Bug: 1274376~~
Change-Id: Iffd610a95199826fea56d7f23cb8e344657631d3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3313692
Reviewed-by: Lei Zhang <thestig@chromium.org>
Commit-Queue: Daniel Hosseinian <dhoss@chromium.org>
Cr-Commit-Position: refs/heads/main@{#948105}

[modify] https://crrev.com/6d9638366ae0f60f8d2db41857fcbc738c2514d4/pdf/pdf_view_web_plugin.h
[modify] https://crrev.com/6d9638366ae0f60f8d2db41857fcbc738c2514d4/pdf/pdf_view_web_plugin.cc

Comment 15 by dhoss@chromium.org on Fri, Dec 3, 2021, 2:46 PM EST Project Member

Labels: -Target-96 Target-97 Merge-Request-97

This feature hasn't been released to stable on M96, nor do we plan to. Per #c10, we'd like to merge to M97.

Comment 16 by dhoss@chromium.org on Fri, Dec 3, 2021, 2:46 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 17 by sheriffbot on Sat, Dec 4, 2021, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Sat, Dec 4, 2021, 1:40 PM EST Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 19 by sheriffbot on Sat, Dec 4, 2021, 2:41 PM EST Project Member

Labels: -Merge-Request-97 Hotlist-Merge-Review Merge-Review-97

Merge review required: M97 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.

Please contact the milestone owner if you have questions.
Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 20 by dhoss@chromium.org on Mon, Dec 6, 2021, 3:53 PM EST Project Member

1. This is a security issue with a feature we hope to launch in M97.
2. crrev.com/c/3313692
3. Yes
4. Yes, and the experiment is active in Beta.
5. N/A
6. N/A

Comment 21 by amyressler@chromium.org on Mon, Dec 6, 2021, 5:32 PM EST Project Member

Labels: -Merge-Review-97 Merge-Approved-97

merge approved for M97; please merge to branch 4692 ASAP/ NTL 12pm PST tomorrow (Tuesday, 7 DEC) so this fix can be included in tomorrow's beta cut

Comment 22 by pbommana@google.com on Tue, Dec 7, 2021, 12:07 PM EST Project Member

Your change has been approved for M97 branch 4692,please go ahead and merge the CL's to M97 branch manually asap so that they would be part of tomorrows Beta release.thank you

Comment 23 by dhoss@chromium.org on Tue, Dec 7, 2021, 12:25 PM EST Project Member

The merge CL is crrev.com/c/3319376. I've been trying to get it through a flaky mac-rel bot since yesterday. I'll try again now.

Comment 24 by Git Watcher on Tue, Dec 7, 2021, 7:33 PM EST Project Member

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7fabaa4d4eea71886dd30962dc96aa0f59bd73e3

commit 7fabaa4d4eea71886dd30962dc96aa0f59bd73e3
Author: Daniel Hosseinian <dhoss@chromium.org>
Date: Wed Dec 08 00:32:35 2021

[M97][unseasoned-pdf] Call PdfViewWebPlugin a11y methods asyncly

Calling a11y methods asyncly protects against the self-deletions they
may cause. The a11y methods call
content::RenderAccessibility::GenerateAXID() underneath, which may
cause a relayout which causes the PdfViewWebPlugin to be deleted.

Isolating the calls in posted tasks is a clean way to protect against
continuing control flow in the object after it is deleted.

(cherry picked from commit 6d9638366ae0f60f8d2db41857fcbc738c2514d4)

~~Bug: 1274376~~
Change-Id: Iffd610a95199826fea56d7f23cb8e344657631d3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3313692

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3313692
Reviewed-by: Lei Zhang <thestig@chromium.org>
Commit-Queue: Daniel Hosseinian <dhoss@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#948105}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3319376
Auto-Submit: Daniel Hosseinian <dhoss@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#799}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify] https://crrev.com/7fabaa4d4eea71886dd30962dc96aa0f59bd73e3/pdf/pdf_view_web_plugin.h
[modify] https://crrev.com/7fabaa4d4eea71886dd30962dc96aa0f59bd73e3/pdf/pdf_view_web_plugin.cc

Comment 25 by amyressler@chromium.org on Tue, Jan 4, 2022, 11:53 AM EST Project Member

Labels: Release-0-M97

Comment 26 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0105 CVE_description-missing

Comment 27 by amyressler@google.com on Wed, Jan 5, 2022, 8:02 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-5000

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 28 by amyressler@chromium.org on Wed, Jan 5, 2022, 8:34 PM EST Project Member

Congratulations, Cassidy Kim! The VRP Panel has decided to award you $5,000 for this report. Nice work!

Comment 29 by amyressler@google.com on Thu, Jan 6, 2022, 3:50 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 30 by sheriffbot on Sat, Mar 12, 2022, 1:29 PM EST Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 31 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by hanleyt@google.com on Wed, Oct 5, 2022, 1:56 PM EDT Project Member

Status: Verified (was: Fixed)

Error for uaf in chrome_pdf::PdfViewPluginBase::LoadAccessibility no longer being reported. Issue presumed fixed.