Starred by 2 users

Owner:	caseq@chromium.org
CC:	yangguo@chromium.org sigurds@chromium.org dsv@google.com
Status:	Fixed *(Closed)*
Components:	Platform>DevTools
Modified:	Sep 9, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

reward-10000
Security_Impact-Stable
Hotlist-Merge-Approved
Security_Severity-High
ReleaseBlock-Stable
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-91
Target-91
Target-92
external_security_report
FoundIn-92
LTS-Security-90
LTS-Security-NotApplicable-90
merge-merged-4515
merge-merged-92
Release-0-M92
CVE-2021-30567

Issue 1211326: SUMMARY: AddressSanitizer: heap-use-after-free devtools_agent_host_impl.h:84 in std::__1::vector<content::protocol::TargetHandler*, std::__1::allocator<content::protocol::TargetHandler*> > content::DevToolsAgentHostImpl::HandlersByName<content::protocol::TargetHandler>(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&)

Reported by dmitr...@gmail.com on Thu, May 20, 2021, 8:14 AM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:78.0) Gecko/20100101 Firefox/78.0

Steps to reproduce the problem:
1. Open Chromium.
2. Open Developer Tools from homepage.
3. Hold Command (or Ctrl) + R until crash of Chromium

What is the expected behavior?
Page reloaded but Chromium do not crash with heap-use-after-free.

What went wrong?
Looks like, Developer Tools try to access non-existent session which discarded with call to "content::RenderFrameHostManager::DiscardUnusedFrame" and it's lead to heap-use-after-free on looped reload of page.

Heap UaF triggered by method DevToolsAgentHostImpl::HandlersByName[1]

[1] https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/content/browser/devtools/devtools_agent_host_impl.h#82

Check attachments for video with reproduction.

ASAN Crash log:

```
==75341==ERROR: AddressSanitizer: heap-use-after-free on address 0x6150005a91a8 at pc 0x00011bbdda11 bp 0x7ffee601b250 sp 0x7ffee601b248
READ of size 8 at 0x6150005a91a8 thread T0
==75341==WARNING: Can't read from symbolizer at fd 111
==75341==WARNING: Can't read from symbolizer at fd 112
==75341==WARNING: Can't read from symbolizer at fd 113
==75341==WARNING: Can't read from symbolizer at fd 114
==75341==WARNING: Failed to use and restart external symbolizer!
    #0 0x11bbdda10 in std::__1::vector<content::protocol::TargetHandler*, std::__1::allocator<content::protocol::TargetHandler*> >
content::DevToolsAgentHostImpl::HandlersByName<content::protocol::TargetHandler>(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >
const&)+0x3e0 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bc0a10)
    #1 0x11bbdd50b in content::protocol::TargetHandler::ForAgentHost(content::DevToolsAgentHostImpl*)+0x1eb (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bc050b)
    #2 0x11bc1def2 in content::RenderFrameDevToolsAgentHost::DidFinishNavigation(content::NavigationHandle*)+0x152 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-
mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4c00ef2)
    #3 0x11ca08b97 in void content::WebContentsImpl::WebContentsObserverList::NotifyObservers<void (content::WebContentsObserver::*)(content::NavigationHandle*),
content::NavigationHandle*&>(void (content::WebContentsObserver::*)(content::NavigationHandle*), content::NavigationHandle*&)+0x667
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x59ebb97)
    #4 0x11ca09eaf in content::WebContentsImpl::DidFinishNavigation(content::NavigationHandle*)+0x13f (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
```

881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x59eceaf)
    #5 0x11c418e06 in content::NavigationRequest::~NavigationRequest()+0x516 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x53fbe06)
    #6 0x11c41b75d in content::NavigationRequest::~NavigationRequest()+0xd (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x53fe75d)
    #7 0x11c51e085 in std::__1::__tree<std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest,
std::__1::default_delete<content::NavigationRequest> > >, std::__1::__map_value_compare<content::NavigationRequest*,
std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest, std::__1::default_delete<content::NavigationRequest> > >,
std::__1::less<content::NavigationRequest*>, true>, std::__1::allocator<std::__1::__value_type<content::NavigationRequest*,
std::__1::unique_ptr<content::NavigationRequest, std::__1::default_delete<content::NavigationRequest> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest,
std::__1::default_delete<content::NavigationRequest> > >, void*>*)+0xa5 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x5501085)
    #8 0x11c4956df in content::RenderFrameHostImpl::~RenderFrameHostImpl()+0x70f (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x54786df)
    #9 0x11c49a42d in content::RenderFrameHostImpl::~RenderFrameHostImpl()+0xd (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x547d42d)
    #10 0x11c54bd17 in content::RenderFrameHostManager::DiscardUnusedFrame(std::__1::unique_ptr<content::RenderFrameHostImpl,
std::__1::default_delete<content::RenderFrameHostImpl> >)+0x4d7 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x552ed17)
    #11 0x11c5452da in content::RenderFrameHostManager::CleanUpNavigation()+0x14a (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x55282da)
    #12 0x11c4b737e in content::RenderFrameHostImpl::StartPendingDeletionOnSubtree()+0xee (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x549a37e)
    #13 0x11c4b71c6 in content::RenderFrameHostImpl::Detach()+0x146 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x549a1c6)
    #14 0x1199cd240 in blink::mojom::LocalFrameHostStubDispatch::Accept(blink::mojom::LocalFrameHost*, mojo::Message*)+0x3900
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x29b0240)
    #15 0x124822339 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)+0x649 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd805339)
    #16 0x12483007e in mojo::MessageDispatcher::Accept(mojo::Message*)+0x27e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd81307e)
    #17 0x12669f0ec in IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptOnProxyThread(mojo::Message)+0x22c
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xf6820ec)
    #18 0x126697d0c in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message),
scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>, void ()>::RunOnce(base::internal::BindStateBase*)+0x16c
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xf67ad0c)
    #19 0x123079419 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*)+0x3e9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc05c419)
    #20 0x1230b8582 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)+0x502
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xc09b582)
    #21 0x1230b7d67 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x1f7 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-
release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc09ad67)
    #22 0x1231a7938 in invocation function for block in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0xe8 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-
mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc18a938)
    #23 0x123194359 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc177359)
    #24 0x1231a60e5 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0x175 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc1890e5)
    #25 0x7fff204a7a0b in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x81a0b)
    #26 0x7fff204a7973 in __CFRunLoopDoSource0+0xb3 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x81973)
    #27 0x7fff204a76ee in __CFRunLoopDoSources0+0xf7 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x816ee)
    #28 0x7fff204a6120 in __CFRunLoopRun+0x379 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x80120)
    #29 0x7fff204a56cd in CFRunLoopRunSpecific+0x232 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x7f6cd)
    #30 0x7fff2872d62f in RunCurrentEventLoopInMode+0x123
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_64+0x3162f)
    #31 0x7fff2872d42b in ReceiveNextEventCommon+0x2c4
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_64+0x3142b)
    #32 0x7fff2872d14e in _BlockUntilNextEventMatchingListInModeWithFilter+0x3f
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_64+0x3114e)
    #33 0x7fff22cc59b0 in _DPSNextEvent+0x372 (/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x3e9b0)
    #34 0x7fff22cc4176 in -[NSApplication(NSEvent) _nextEventMatchingEventMask:untilDate:inMode:dequeue:]+0x555
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x3d176)
    #35 0x124367cc2 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke+0x192
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xd34acc2)
    #36 0x123194359 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc177359)
    #37 0x12436785a in -[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]+0x32a (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd34a85a)
    #38 0x7fff22cb6689 in -[NSApplication run]+0x249 (/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x2f689)
    #39 0x1231a93aa in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*)+0x3da (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc18c3aa)
    #40 0x1231a4f08 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*)+0x208 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc187f08)
    #41 0x1230b97e5 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)+0x2a5
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xc09c7e5)
    #42 0x122ff494e in base::RunLoop::Run(base::Location const&)+0x46e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xbfd794e)
    #43 0x11b862985 in content::BrowserMainLoop::RunMainMessageLoop()+0x265 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4845985)
    #44 0x11b866f11 in content::BrowserMainRunnerImpl::Run()+0x31 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4849f11)
    #45 0x11b85be5c in content::BrowserMain(content::MainFunctionParams const&)+0x37c (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x483ee5c)
    #46 0x122dbe522 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool)+0xb62 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-
release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xbda1522)
    #47 0x122dbd7c6 in content::ContentMainRunnerImpl::Run(bool)+0x426 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xbda07c6)
    #48 0x122dbaa97 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*)+0x1647
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xbd9da97)
    #49 0x122dbb0cc in content::ContentMain(content::ContentMainParams const&)+0x1c (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xbd9e0cc)
    #50 0x117023345 in ChromeMain+0x225 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x6345)
    #51 0x109be0e9f in main+0x1ff (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/MacOS/./Chromium:x86_64+0x100003e9f)

```
    #52 0x7fff203ca620 in start+0x0 (/usr/lib/system/libdyld.dylib:x86_64+0x15620)

0x6150005a91a8 is located 40 bytes inside of 504-byte region [0x6150005a9180,0x6150005a9378)
freed by thread T0 here:
    #0 0x109dda039 in __asan_memmove+0x1d19 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/MacOS/libclang_rt.asan_osx_dynamic.dylib:x86_64+0x45039)
    #1 0x11bc1e2d3 in content::RenderFrameDevToolsAgentHost::DidFinishNavigation(content::NavigationHandle*)+0x533 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-
mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4c012d3)
    #2 0x11ca08b97 in void content::WebContentsImpl::WebContentsObserverList::NotifyObservers<void (content::WebContentsObserver::*)(content::NavigationHandle*),
content::NavigationHandle*&>(void (content::WebContentsObserver::*)(content::NavigationHandle*), content::NavigationHandle*&)+0x667
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x59ebb97)
    #3 0x11ca09eaf in content::WebContentsImpl::DidFinishNavigation(content::NavigationHandle*)+0x13f (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x59eceaf)
    #4 0x11c418e06 in content::NavigationRequest::~NavigationRequest()+0x516 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x53fbe06)
    #5 0x11c41b75d in content::NavigationRequest::~NavigationRequest()+0xd (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x53fe75d)
    #6 0x11c51e085 in std::__1::__tree<std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest,
std::__1::default_delete<content::NavigationRequest> > >, std::__1::__map_value_compare<content::NavigationRequest*,
std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest, std::__1::default_delete<content::NavigationRequest> > >,
std::__1::less<content::NavigationRequest*>, true>, std::__1::allocator<std::__1::__value_type<content::NavigationRequest*,
std::__1::unique_ptr<content::NavigationRequest, std::__1::default_delete<content::NavigationRequest> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<content::NavigationRequest*, std::__1::unique_ptr<content::NavigationRequest,
std::__1::default_delete<content::NavigationRequest> > >, void*>*)+0xa5 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x5501085)
    #7 0x11c4956df in content::RenderFrameHostImpl::~RenderFrameHostImpl()+0x70f (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x54786df)
    #8 0x11c49a42d in content::RenderFrameHostImpl::~RenderFrameHostImpl()+0xd (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x547d42d)
    #9 0x11c54bd17 in content::RenderFrameHostManager::DiscardUnusedFrame(std::__1::unique_ptr<content::RenderFrameHostImpl,
std::__1::default_delete<content::RenderFrameHostImpl> >)+0x4d7 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x552ed17)
    #10 0x11c5452da in content::RenderFrameHostManager::CleanUpNavigation()+0x14a (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x55282da)
    #11 0x11c4b737e in content::RenderFrameHostImpl::StartPendingDeletionOnSubtree()+0xee (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x549a37e)
    #12 0x11c4b71c6 in content::RenderFrameHostImpl::Detach()+0x146 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x549a1c6)
    #13 0x1199cd240 in blink::mojom::LocalFrameHostStubDispatch::Accept(blink::mojom::LocalFrameHost*, mojo::Message*)+0x3900
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x29b0240)
    #14 0x124822339 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)+0x649 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd805339)
    #15 0x12483007e in mojo::MessageDispatcher::Accept(mojo::Message*)+0x27e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd81307e)
    #16 0x12669f0ec in IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptOnProxyThread(mojo::Message)+0x22c
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xf6820ec)
    #17 0x126697d0c in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message),
scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>, void ()>::RunOnce(base::internal::BindStateBase*)+0x16c
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xf67ad0c)
    #18 0x123079419 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*)+0x3e9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc05c419)
    #19 0x1230b8582 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)+0x502
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0xc09b582)
    #20 0x1230b7d67 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x1f7 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-
release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc09ad67)
    #21 0x1231a7938 in invocation function for block in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0xe8 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-
mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc18a938)
    #22 0x123194359 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc177359)
    #23 0x1231a60e5 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0x175 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc1890e5)
    #24 0x7fff204a7a0b in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x81a0b)
    #25 0x7fff204a7973 in __CFRunLoopDoSource0+0xb3 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x81973)
    #26 0x7fff204a76ee in __CFRunLoopDoSources0+0xf7 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x816ee)
    #27 0x7fff204a6120 in __CFRunLoopRun+0x379 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x80120)
    #28 0x7fff204a56cd in CFRunLoopRunSpecific+0x232 (/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64h+0x7f6cd)
    #29 0x7fff2872d62f in RunCurrentEventLoopInMode+0x123
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_64+0x3162f)

previously allocated by thread T0 here:
    #0 0x109dd9ef0 in __asan_memmove+0x1bd0 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/MacOS/libclang_rt.asan_osx_dynamic.dylib:x86_64+0x44ef0)
    #1 0x122eedc77 in operator new(unsigned long)+0x27 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xbed0c77)
    #2 0x11bc18dc8 in content::RenderFrameDevToolsAgentHost::CreateForLocalRootOrPortalNavigation(content::NavigationRequest*)+0x38
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x4bfbdc8)
    #3 0x11bbccd98 in content::protocol::TargetAutoAttacher::AutoAttachToFrame(content::NavigationRequest*, bool)+0x178 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-
mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bafd98)
    #4 0x11bbf5150 in content::protocol::TargetHandler::ResponseThrottle::MaybeThrottle()+0x180 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bd8150)
    #5 0x11bbf4fbd in content::protocol::TargetHandler::ResponseThrottle::WillProcessResponse()+0xd (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bd7fbd)
    #6 0x11c46c28d in content::NavigationThrottleRunner::ProcessInternal()+0x46d (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x544f28d)
    #7 0x11c436b0c in content::NavigationRequest::WillProcessResponse()+0x14c (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x5419b0c)
    #8 0x11c4346c9 in content::NavigationRequest::OnResponseStarted(mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>,
mojo::StructPtr<network::mojom::URLResponseHead>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID, bool,
blink::NavigationDownloadPolicy, net::NetworkIsolationKey, base::Optional<content::SubresourceLoaderParams>,
content::NavigationURLLoaderDelegate::EarlyHints)+0x3629 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-
881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x54176c9)
    #9 0x11bfb15a5 in content::NavigationURLLoaderImpl::NotifyResponseStarted(mojo::StructPtr<network::mojom::URLResponseHead>,
mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID const&, bool)+0x585
(/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium
Framework:x86_64+0x4f945a5)
    #10 0x11bfbc14a in void base::internal::FunctorTraits<void (content::NavigationURLLoaderImpl::*)(mojo::StructPtr<network::mojom::URLResponseHead>,
```

mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID const&, bool), void>::Invoke<void (content::NavigationURLLoaderImpl::*)(mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID const&, bool), base::WeakPtr<content::NavigationURLLoaderImpl>, mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID, bool>(void (content::NavigationURLLoaderImpl::*) (mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID const&, bool), base::WeakPtr<content::NavigationURLLoaderImpl>&&, mojo::StructPtr<network::mojom::URLResponseHead>&&, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>&&, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>&&, content::GlobalRequestID&&, bool&&)+0x28a (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4f9f14a)

#11 0x11bfbbe9b in base::internal::Invoker<base::internal::BindState<void (content::NavigationURLLoaderImpl::*)(mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID const&, bool), base::WeakPtr<content::NavigationURLLoaderImpl>, mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, content::GlobalRequestID, bool>, void ()>::RunOnce(base::internal::BindStateBase*)+0x8b (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4f9ee9b)

#12 0x11bfb1abe in content::NavigationURLLoaderImpl::ParseHeaders(GURL const&, network::mojom::URLResponseHead*, base::OnceCallback<void ()>)+0x13e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4f94abe)

#13 0x11bfb0e68 in content::NavigationURLLoaderImpl::CallOnReceivedResponse(mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>, bool)+0x408 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4f93e68)

#14 0x11bfaeffb in content::NavigationURLLoaderImpl::OnStartLoadingResponseBody(mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>)+0x61b (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4f91ffb)

#15 0x119ecc2ee in blink::ThrottlingURLLoader::OnStartLoadingResponseBody(mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>)+0x16e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x2eaf2ee)

#16 0x1189d055c in network::mojom::URLLoaderClientStubDispatch::Accept(network::mojom::URLLoaderClient*, mojo::Message*)+0x8fc (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x19b355c)

#17 0x124822339 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)+0x649 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd805339)

#18 0x124830165 in mojo::MessageDispatcher::Accept(mojo::Message*)+0x365 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd813165)

#19 0x12483c5b9 in mojo::internal::MultiplexRouter::ProcessIncomingMessage(mojo::internal::MultiplexRouter::MessageWrapper*, mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*)+0x809 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd81f5b9)

#20 0x12483aa93 in mojo::internal::MultiplexRouter::Accept(mojo::Message*)+0x5e3 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd81da93)

#21 0x124830165 in mojo::MessageDispatcher::Accept(mojo::Message*)+0x365 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd813165)

#22 0x1248173a4 in mojo::Connector::DispatchMessage(mojo::Message)+0x384 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd7fa3a4)

#23 0x1248190e8 in mojo::Connector::ReadAllAvailableMessages()+0x268 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd7fc0e8)

#24 0x12488425e in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&)+0x36e (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd86725e)

#25 0x12488533a in base::internal::Invoker<base::internal::BindState<void (mojo::SimpleWatcher::*)(int, unsigned int, mojo::HandleSignalsState const&), base::WeakPtr<mojo::SimpleWatcher>, int, unsigned int, mojo::HandleSignalsState>, void ()>::RunOnce(base::internal::BindStateBase*)+0x21a (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xd86833a)

#26 0x123079419 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*)+0x3e9 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc05c419)

#27 0x1230b8582 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)+0x502 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc09b582)

#28 0x1230b7d67 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x1f7 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc09ad67)

#29 0x1231a7938 in invocation function for block in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0xe8 (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0xc18a938)

SUMMARY: AddressSanitizer: heap-use-after-free (/Users/ddv_ua/InfoSec/Apps/Chromium/asan-mac-release-881922/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/92.0.4506.0/Chromium Framework:x86_64+0x4bc0a10) in std::__1::vector<content::protocol::TargetHandler*, std::__1::allocator<content::protocol::TargetHandler*> > content::DevToolsAgentHostImpl::HandlersByName<content::protocol::TargetHandler>(std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&)+0x3e0

Shadow bytes around the buggy address:
  0x1c2a000b51e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b51f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5200: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5210: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5220: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x1c2a000b5230: fd fd fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5240: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5250: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c2a000b5260: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fa
  0x1c2a000b5270: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c2a000b5280: 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
==75341==ABORTING
Received signal 6
 [0x00012316c6c9]
 [0x000122f15a63]
 [0x00012316c44b]

[0x7fff203f3d7d]
[0x000109e31000]
[0x7fff20302720]
[0x000109df9856]
[0x000109df8f84]
[0x000109de0604]
[0x000109ddfeda]
[0x000109de0ad8]
[0x00011bbdda11]
[0x00011bbdd50c]
[0x00011bc1def3]
[0x00011ca08b98]
[0x00011ca09eb0]
[0x00011c418e07]
[0x00011c41b75e]
[0x00011c51e086]
[0x00011c4956e0]
[0x00011c49a42e]
[0x00011c54bd18]
[0x00011c5452db]
[0x00011c4b737f]
[0x00011c4b71c7]
[0x0001199cd241]
[0x00012482233a]
[0x00012483007f]
[0x00012669f0ed]
[0x000126697d0d]
[0x00012307941a]
[0x0001230b8583]
[0x0001230b7d68]
[0x0001231a7939]
[0x00012319435a]
[0x0001231a60e6]
[0x7fff204a7a0c]
[0x7fff204a7974]
[0x7fff204a76ef]
[0x7fff204a6121]
[0x7fff204a56ce]
[0x7fff2872d630]
[0x7fff2872d42c]
[0x7fff2872d14f]
[0x7fff22cc59b1]
[0x7fff22cc4177]
[0x000124367cc3]
[0x00012319435a]
[0x00012436785b]
[0x7fff22cb668a]
[0x0001231a93ab]
[0x0001231a4f09]
[0x0001230b97e6]
[0x000122ff494f]
[0x00011b862986]
[0x00011b866f12]
[0x00011b85be5d]
[0x000122dbe523]
[0x000122dbd7c7]
[0x000122dbaa98]
[0x000122dbb0cd]
[0x000117023346]
[0x000109be0ea0]
[0x7fff203ca621]
[0x000000000002]
[end of stack trace]

Did this work before? N/A

Chrome version: 92.0.4506.0 (Developer Build) (x86_64) Channel: n/a
OS Version: OS X 10.15
Flash Version: Shockwave Flash 30.0 r0

ChromiumHeapUaFViaLoopedReloadWithDevTools.mp4
1.6 MB View Download

Comment 1 by sheriffbot on Thu, May 20, 2021, 8:19 AM EDT Project Member

Labels: external_security_report

Comment 2 by vakh@chromium.org on Fri, May 21, 2021, 2:04 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: caseq@chromium.org
Cc: alph@chromium.org sigurds@chromium.org yangguo@chromium.org
Components: Platform>DevTools

Comment 3 by vakh@chromium.org on Fri, May 21, 2021, 2:06 PM EDT Project Member

Labels: Security_Impact-Head

Setting Security_Impact-Head based on the report. I'll try to reproduce this locally.

Comment 4 by vakh@chromium.org on Sat, May 22, 2021, 3:59 AM EDT Project Member

FWIW, I couldn't reproduce it on Linux and Chrome OS. Haven't been able to try MacOS yet.

Comment 5 by dmitr...@gmail.com on Sat, May 22, 2021, 3:38 PM EDT

Hello again,

1. I tried to reproduce this in Debian 10 with latest available version of Linux kernel (running on virtual machine), but Heap UaF don't triggered with same scenario. Anyway, maybe, I used wrong Chromium build, so can't be sure if this is don't work for Linux.
2. This worked for me in MacOS (version 11.2.3) and Windows (8.1). I attach ASAN report from Windows to this comment as proof. I used Chromium version referenced in report (92.0.4506.0 (Developer Build)) for this tests.

Thanks.

win-asan-report-heap-uaf.txt
17.9 KB View Download

Comment 6 by adetaylor@google.com on Wed, May 26, 2021, 1:46 PM EDT Project Member

Labels: Security_Severity-High

Reproduced on Mac ASAN release 881922. I'm going to try on an older build to get the security impact label right.

As for severity, as a browser process UaF this would normally be Critical. It's presumably mitigated by the need to have devtools open. It's not clear if this can be triggered by remote content, but I'm going to assume High severity.

Comment 7 by adetaylor@google.com on Wed, May 26, 2021, 1:50 PM EDT Project Member

Doesn't happen on Mac ASAN release 870757.

Comment 8 by adetaylor@google.com on Wed, May 26, 2021, 1:52 PM EDT Project Member

Labels: -Security_Impact-Head Security_Impact-Beta

As 881922 is between M91 and M92, and this doesn't appear with the ASAN build corresponding to (roughly) the branch point of M91, I'm going to assume this is an M92 regression and therefore Security_Impact-Beta.

Comment 9 by caseq@chromium.org on Thu, May 27, 2021, 1:09 AM EDT Project Member

Status: Started (was: Assigned)
Cc: -alph@chromium.org
Labels: foundin-92 Target-92 OS-Chrome OS-Fuchsia OS-Linux OS-Windows

The fix is on its way: https://chromium-review.googlesource.com/c/chromium/src/+/2920730
This is regressed by this: https://chromium-review.googlesource.com/c/chromium/src/+/2826852 (so, yes, m92)

Comment 10 by sheriffbot on Thu, May 27, 2021, 12:58 PM EDT Project Member

Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Beta and high severity.

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

Comment 11 by sheriffbot on Thu, May 27, 2021, 1:19 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 12 by sheriffbot on Thu, May 27, 2021, 1:29 PM EDT Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 13 by Git Watcher on Fri, May 28, 2021, 1:23 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3ee01e4fd442a1d6563e79be86d66c83a087cfb0

commit 3ee01e4fd442a1d6563e79be86d66c83a087cfb0
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Fri May 28 05:22:20 2021

Fix a UAF in RenderFrameDevToolsAgentHost

Originally regressed by https://crrev.com/c/2826852

~~Bug: 1211226~~
Change-Id: I6f639862ea25f5d7ef745864c38a0f1e96dbb3e0
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2920730
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
Reviewed-by: Yang Guo <yangguo@chromium.org>
Cr-Commit-Position: refs/heads/master@{#887464}

[modify] https://crrev.com/3ee01e4fd442a1d6563e79be86d66c83a087cfb0/content/browser/devtools/render_frame_devtools_agent_host.cc
[add] https://crrev.com/3ee01e4fd442a1d6563e79be86d66c83a087cfb0/third_party/blink/web_tests/http/tests/inspector-protocol/page/reload-with-oopifs-crash-expected.txt
[add] https://crrev.com/3ee01e4fd442a1d6563e79be86d66c83a087cfb0/third_party/blink/web_tests/http/tests/inspector-protocol/page/reload-with-oopifs-crash.js

Comment 14 by sheriffbot on Fri, May 28, 2021, 12:21 PM EDT Project Member

Labels: -Security_Impact-Beta Security_Impact-Stable

Comment 15 by caseq@chromium.org on Tue, Jun 1, 2021, 1:05 PM EDT Project Member

Status: Fixed (was: Started)
Labels: -M-91 -Target-91 Merge-Request-92

Removing m91 related labels, as this is not an issue prior to commit referenced in #9. Requesting merge to m92, see #13 for the fix.

Comment 16 by sheriffbot on Tue, Jun 1, 2021, 2:01 PM EDT Project Member

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

Comment 17 by sheriffbot on Wed, Jun 2, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 18 by sheriffbot on Wed, Jun 2, 2021, 12:47 PM EDT Project Member

Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 19 by sheriffbot on Wed, Jun 2, 2021, 1:11 PM EDT Project Member

Labels: -Merge-Request-92 Hotlist-Merge-Approved Merge-Approved-92

Your change meets the bar and is auto-approved for M92. Please go ahead and merge the CL to branch 4515 (refs/branch-heads/4515) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: govind@(Android), bindusuvarna@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 20 by Git Watcher on Wed, Jun 2, 2021, 3:35 PM EDT Project Member

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5a63c928d01e2f4de4ff431ff594f2ee0aeae392

commit 5a63c928d01e2f4de4ff431ff594f2ee0aeae392
Author: Andrey Kosyakov <caseq@chromium.org>
Date: Wed Jun 02 19:34:31 2021

[m92 merge] Fix a UAF in RenderFrameDevToolsAgentHost

Originally regressed by https://crrev.com/c/2826852

(cherry picked from commit 3ee01e4fd442a1d6563e79be86d66c83a087cfb0)

~~Bug: 1211326~~
Change-Id: I6f639862ea25f5d7ef745864c38a0f1e96dbb3e0
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2920730
Commit-Queue: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Dmitry Gozman <dgozman@chromium.org>
Reviewed-by: Yang Guo <yangguo@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#887464}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2934361
Auto-Submit: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Peter Kvitek <kvitekp@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#251}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/5a63c928d01e2f4de4ff431ff594f2ee0aeae392/content/browser/devtools/render_frame_devtools_agent_host.cc
[add] https://crrev.com/5a63c928d01e2f4de4ff431ff594f2ee0aeae392/third_party/blink/web_tests/http/tests/inspector-protocol/page/reload-with-oopifs-crash-expected.txt
[add] https://crrev.com/5a63c928d01e2f4de4ff431ff594f2ee0aeae392/third_party/blink/web_tests/http/tests/inspector-protocol/page/reload-with-oopifs-crash.js

Comment 21 by amyressler@google.com on Thu, Jun 10, 2021, 12:32 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-10000

*** 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 22 by amyressler@chromium.org on Thu, Jun 10, 2021, 12:47 PM EDT Project Member

Congratulations - the VRP Panel has decided to award you $10,000 for this report. Great work!

Comment 23 by amyressler@google.com on Mon, Jun 14, 2021, 11:23 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 24 by amyressler@chromium.org on Mon, Jul 19, 2021, 3:11 PM EDT Project Member

Labels: Release-0-M92

Comment 25 by amyressler@google.com on Mon, Jul 19, 2021, 7:14 PM EDT Project Member

Labels: CVE-2021-30567 CVE_description-missing

Comment 26 by voit@google.com on Wed, Jul 28, 2021, 5:08 AM EDT Project Member

Labels: LTS-Security-NotApplicable-90

M91 regression therefore not applicable for M90 LTS.

Comment 27 by voit@google.com on Wed, Jul 28, 2021, 5:39 AM EDT Project Member

Labels: LTS-Security-90

Comment 28 by amyressler@google.com on Tue, Aug 3, 2021, 3:41 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 29 by sheriffbot on Thu, Sep 9, 2021, 1:30 PM EDT 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