

☆ Starred by 3 users

Owner:

CC:

Status:

Components:

Modified:

Backlog-Rank:

Editors:

EstimatedDays:


NextAction:


OS:


Pri:

Type:

lukasza@chromium.org

 benmason@chromium.org

 pbomm...@chromium.org

 mmenke@chromium.org

sporeba@google.com

stefanoduo@google.com

Fixed (Closed)

Internals>Network

Jun 11, 2021

Linux

1

Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
allpublic
reward-inprocess
Unreproducible
reward-15000
Via-Wizard-Security
CVE_description-submitted
M-89
Target-89
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
Release-0-M89
external_security_report
merge-merged-4389
merge-merged-89
CVE-2021-21179

Issue 1174943: uaf in DestroyURLLoader(network::cors::CorsURLLoaderFactory)

Reported by emily...@gmail.com on Fri, Feb 5, 2021, 1:49 AM EST

 Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.146 Safari/537.36

Steps to reproduce the problem:
os:ubuntu 20.04
Chromium 89.0.4350.4 with asan build
Chromium 90.0.4409.0 with asan build

1 ./chrome -user-data-dir=/tmp/xx http://localhost:8000/crash.html
2 Allow popup window
3 And Press "ctrl + C" repeatedly to force close the browser.

What is the expected behavior?

What went wrong?
==95115==ERROR: AddressSanitizer: heap-use-after-free on address 0x60400004f22c at pc 0x5608abd2de55 bp 0x7fae7b6d0d10 sp 0x7fae7b6d0d08
READ of size 4 at 0x60400004f22c thread T3 (Chrome_ChildIOT)
error: unknown argument '-demangle=True'
#0 0x5608abd2de54 in network::NetworkContext::LoaderDestroyed(unsigned int) ./././buildtools/third_party/libc++/trunk/include/_functional_base:54
#1 0x5608abd2de54 in operator() ./././buildtools/third_party/libc++/trunk/include/map:516
#2 0x5608abd2de54 in __lower_bound<unsigned int> ./././buildtools/third_party/libc++/trunk/include/_tree:2634
#3 0x5608abd2de54 in find<unsigned int> ./././buildtools/third_party/libc++/trunk/include/_tree:2563
#4 0x5608abd2de54 in find ./././buildtools/third_party/libc++/trunk/include/map:1378
#5 0x5608abd2de54 in LoaderDestroyed ./././services/network/network_context.cc:710
#6 0x5608abd2de54 in ?? ???:0
#7 0x5608abe15834 in network::cors::CorsURLLoaderFactory::DestroyURLLoader(network::mojom::URLLoader*)
./././services/network/cors/cors_url_loader_factory.cc:233
#8 0x5608abe15834 in ?? ???:0
#9 0x5608abef5b3e in network::URLLoader::NotifyCompleted(int) ./././base/callback.h:101
#10 0x5608abef5b3e in DeleteSelf ./././services/network/url_loader.cc:1863
#11 0x5608abef5b3e in NotifyCompleted ./././services/network/url_loader.cc:1824
#12 0x5608abef5b3e in ?? ???:0
#13 0x5608abf00976 in network::URLLoader::OnResponseStarted(net::URLRequest*, int) ./././services/network/url_loader.cc:1263
#14 0x5608abf00976 in ?? ???:0
#15 0x5608abd47ae in net::URLRequestHttpJob::OnStartCompleted(int) ./././net/url_request/url_request_http_job.cc:931
#16 0x5608abd47ae in ?? ???:0
#17 0x5608a7f19f0a in net::HttpCache::Transaction::DoLoop(int) ./././base/callback.h:101
#18 0x5608a7f19f0a in DoLoop ./././net/http/http_cache_transaction.cc:1006
#19 0x5608a7f19f0a in ?? ???:0
#20 0x5608a7f351bb in base::internal::Invoker<base::internal::BindState<void (net::HttpCache::Transaction::*)(int), base::WeakPtr<net::HttpCache::Transaction> >, void (int)>::Run(base::internal::BindStateBase*, int) ./././base/bind_internal.h:498
#21 0x5608a7f351bb in MakeItSo<void (net::HttpCache::Transaction::*)(const &)(int), const base::WeakPtr<net::HttpCache::Transaction> &, int>
./././base/bind_internal.h:657
#22 0x5608a7f351bb in RunImpl<void (net::HttpCache::Transaction::*)(const &)(int), const std::tuple<base::WeakPtr<net::HttpCache::Transaction> > &, 0>
./././base/bind_internal.h:710

```
#23 0x5608a7f351bb in Run J.J./base/bind_internal.h:692
#24 0x5608a7f351bb in ?? ???:0
#25 0x5608a7f07775 in net::HttpCache::ProcessEntryFailure(net::HttpCache::ActiveEntry*) J.J./base/callback.h:168
#26 0x5608a7f07775 in ProcessEntryFailure J.J./net/http/http_cache.cc:1058
#27 0x5608a7f07775 in ?? ???:0
#28 0x5608a7f0713e in net::HttpCache::DoneWithEntry(net::HttpCache::ActiveEntry*, net::HttpCache::Transaction*, bool, bool) http_cache.cc:7
#29 0x5608a7f0713e in ?? ???:0
#30 0x5608a7f17413 in net::HttpCache::Transaction::DoneWithEntry(bool) J.J./net/http/http_cache_transaction.cc:3212
#31 0x5608a7f17413 in ?? ???:0
#32 0x5608a7f14e02 in net::HttpCache::Transaction::~Transaction() J.J./net/http/http_cache_transaction.cc:215
#33 0x5608a7f14e02 in ?? ???:0
#34 0x5608a7f174ed in net::HttpCache::Transaction::~Transaction() J.J./net/http/http_cache_transaction.cc:205
#35 0x5608a7f174ed in ?? ???:0
#36 0x5608abdd10d5 in net::URLRequestHttpJob::DestroyTransaction() J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#37 0x5608abdd10d5 in reset J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#38 0x5608abdd10d5 in DestroyTransaction J.J./net/url_request/url_request_http_job.cc:371
#39 0x5608abdd10d5 in ?? ???:0
#40 0x5608abdd0e99 in net::URLRequestHttpJob::Kill() J.J./net/url_request/url_request_http_job.cc:309
#41 0x5608abdd0e99 in ?? ???:0
#42 0x5608a81c564f in net::URLRequest::DoCancel(int, net::SSLInfo const&) J.J./net/url_request/url_request.cc:721
#43 0x5608a81c564f in ?? ???:0
#44 0x5608a81bd5e9 in net::URLRequest::~URLRequest() J.J./net/url_request/url_request.cc:682
#45 0x5608a81bd5e9 in ~URLRequest J.J./net/url_request/url_request.cc:177
#46 0x5608a81bd5e9 in ?? ???:0
#47 0x5608a81bdf9d in net::URLRequest::~URLRequest() J.J./net/url_request/url_request.cc:168
#48 0x5608a81bdf9d in ?? ???:0
#49 0x5608abef8ea3 in network::URLLoader::~URLLoader() J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#50 0x5608abef8ea3 in reset J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#51 0x5608abef8ea3 in ~unique_ptr J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#52 0x5608abef8ea3 in ~URLLoader J.J./services/network/url_loader.cc:924
#53 0x5608abef8ea3 in ?? ???:0
#54 0x5608abef91cd in network::URLLoader::~URLLoader() J.J./services/network/url_loader.cc:918
#55 0x5608abef91cd in ?? ???:0
#56 0x5608abe1956d in std::__1::__tree<std::__1::unique_ptr<network::mojom::URLLoader, std::__1::default_delete<network::mojom::URLLoader>>,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::mojom::URLLoader, std::__1::default_delete<network::mojom::URLLoader>>>
>::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::mojom::URLLoader, std::__1::default_delete<network::mojom::URLLoader>>, void*>*)
J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#57 0x5608abe1956d in reset J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#58 0x5608abe1956d in ~unique_ptr J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#59 0x5608abe1956d in __destroy<std::unique_ptr<network::mojom::URLLoader> > J.J./buildtools/third_party/libc++/trunk/include/memory:1787
#60 0x5608abe1956d in destroy<std::unique_ptr<network::mojom::URLLoader> > J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#61 0x5608abe1956d in destroy J.J./buildtools/third_party/libc++/trunk/include/_tree:1833
#62 0x5608abe1956d in ?? ???:0
#63 0x5608abe15525 in network::cors::CorsURLLoaderFactory::~CorsURLLoaderFactory() J.J./buildtools/third_party/libc++/trunk/include/_tree:1821
#64 0x5608abe15525 in ~set J.J./buildtools/third_party/libc++/trunk/include/set:603
#65 0x5608abe15525 in ~CorsURLLoaderFactory J.J./services/network/cors/cors_url_loader_factory.cc:222
#66 0x5608abe15525 in ?? ???:0
#67 0x5608abd44af4 in std::__1::__tree<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory, std::__1::default_delete<network::cors::CorsURLLoaderFactory> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> > > >::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> >, void*>*) J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#68 0x5608abd44af4 in reset J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#69 0x5608abd44af4 in ~unique_ptr J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#70 0x5608abd44af4 in __destroy<std::unique_ptr<network::cors::CorsURLLoaderFactory> > J.J./buildtools/third_party/libc++/trunk/include/memory:1787
#71 0x5608abd44af4 in destroy<std::unique_ptr<network::cors::CorsURLLoaderFactory> > J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#72 0x5608abd44af4 in destroy J.J./buildtools/third_party/libc++/trunk/include/_tree:1833
#73 0x5608abd44af4 in ?? ???:0
#74 0x5608abd44aa9 in std::__1::__tree<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory, std::__1::default_delete<network::cors::CorsURLLoaderFactory> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> > > >::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> >, void*>*) J.J./buildtools/third_party/libc++/trunk/include/_tree:1830
#75 0x5608abd44aa9 in ?? ???:0
#76 0x5608abd44aa9 in std::__1::__tree<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory, std::__1::default_delete<network::cors::CorsURLLoaderFactory> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> > > >::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> >, void*>*) J.J./buildtools/third_party/libc++/trunk/include/_tree:1830
#77 0x5608abd44aa9 in ?? ???:0
#78 0x5608abd44aa9 in std::__1::__tree<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory, std::__1::default_delete<network::cors::CorsURLLoaderFactory> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> > > >::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> >, void*>*) J.J./buildtools/third_party/libc++/trunk/include/_tree:1830
#79 0x5608abd44aa9 in ?? ???:0
#80 0x5608abd44aa9 in std::__1::__tree<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory, std::__1::default_delete<network::cors::CorsURLLoaderFactory> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> > > >::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::cors::CorsURLLoaderFactory,
std::__1::default_delete<network::cors::CorsURLLoaderFactory> >, void*>*) J.J./buildtools/third_party/libc++/trunk/include/_tree:1830
#81 0x5608abd44aa9 in ?? ???:0
#82 0x5608abd2a171 in network::NetworkContext::~NetworkContext() J.J./buildtools/third_party/libc++/trunk/include/_tree:1821
#83 0x5608abd2a171 in ~set J.J./buildtools/third_party/libc++/trunk/include/set:603
#84 0x5608abd2a171 in ~NetworkContext J.J./services/network/network_context.cc:534
#85 0x5608abd2a171 in ?? ???:0
#86 0x5608abd2aa7d in network::NetworkContext::~NetworkContext() J.J./services/network/network_context.cc:492
#87 0x5608abd2aa7d in ?? ???:0
#88 0x5608abd0ff1d in std::__1::__tree<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> > >
>::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> >, void*>*)
J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#89 0x5608abd0ff1d in reset J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#90 0x5608abd0ff1d in ~unique_ptr J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#91 0x5608abd0ff1d in __destroy<std::unique_ptr<network::NetworkContext> > J.J./buildtools/third_party/libc++/trunk/include/memory:1787
#92 0x5608abd0ff1d in destroy<std::unique_ptr<network::NetworkContext> > J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#93 0x5608abd0ff1d in destroy J.J./buildtools/third_party/libc++/trunk/include/_tree:1833
#94 0x5608abd0ff1d in ?? ???:0
#95 0x5608abd0fed1 in std::__1::__tree<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> >,
base::UniquePtrComparator, std::__1::allocator<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> > >
>::destroy(std::__1::__tree_node<std::__1::unique_ptr<network::NetworkContext, std::__1::default_delete<network::NetworkContext> >, void*>*)
J.J./buildtools/third_party/libc++/trunk/include/_tree:1831
#96 0x5608abd0fed1 in ?? ???:0
#97 0x5608abd05ae1 in network::NetworkService::~NetworkService() J.J./buildtools/third_party/libc++/trunk/include/_tree:1870
#98 0x5608abd05ae1 in clear J.J./buildtools/third_party/libc++/trunk/include/set:693
#99 0x5608abd05ae1 in DestroyNetworkContexts J.J./services/network/network_service.cc:855
#100 0x5608abd05ae1 in ~NetworkService J.J./services/network/network_service.cc:409
#101 0x5608abd05ae1 in ?? ???:0
```

```
#102 0x5608abd065ed in network::NetworkService::~NetworkService() J.J.J./services/network/network_service.cc:402
#103 0x5608abd065ed in ?? ???
#104 0x5608a54590ee in mojo::ServiceFactory::InstanceHolder<network::mojom::NetworkService>::~InstanceHolder()
J.J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#105 0x5608a54590ee in reset J.J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#106 0x5608a54590ee in ~unique_ptr<J.J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#107 0x5608a54590ee in ~InstanceHolder J.J.J./mojo/public/cpp/bindings/service_factory.h:127
#108 0x5608a54590ee in ~InstanceHolder J.J.J./mojo/public/cpp/bindings/service_factory.h:127
#109 0x5608a54590ee in ?? ???
#110 0x5608a7a497c2 in unsigned long base::internal::flat_tree<std::__1::unique_ptr<mojo::ServiceFactory::InstanceHolderBase,
std::__1::default_delete<mojo::ServiceFactory::InstanceHolderBase> >, base::identity, base::UniquePtrComparator,
std::__1::vector<std::__1::unique_ptr<mojo::ServiceFactory::InstanceHolderBase, std::__1::default_delete<mojo::ServiceFactory::InstanceHolderBase> >,
std::__1::allocator<std::__1::unique_ptr<mojo::ServiceFactory::InstanceHolderBase, std::__1::default_delete<mojo::ServiceFactory::InstanceHolderBase> > > >
>::erase<mojo::ServiceFactory::InstanceHolderBase>(>)(mojo::ServiceFactory::InstanceHolderBase* const&) J.J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#111 0x5608a7a497c2 in reset J.J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#112 0x5608a7a497c2 in ~unique_ptr<J.J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#113 0x5608a7a497c2 in destroy J.J.J./buildtools/third_party/libc++/trunk/include/memory:1920
#114 0x5608a7a497c2 in __destroy<std::unique_ptr<mojo::ServiceFactory::InstanceHolderBase> > J.J.J./buildtools/third_party/libc++/trunk/include/memory:1782
#115 0x5608a7a497c2 in destroy<std::unique_ptr<mojo::ServiceFactory::InstanceHolderBase> > J.J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#116 0x5608a7a497c2 in __destruct_at_end J.J.J./buildtools/third_party/libc++/trunk/include/memory:426
#117 0x5608a7a497c2 in __destruct_at_end J.J.J./buildtools/third_party/libc++/trunk/include/memory:426
#118 0x5608a7a497c2 in erase J.J.J./buildtools/third_party/libc++/trunk/include/memory:1738
#119 0x5608a7a497c2 in erase J.J.J./base/containers/flat_tree.h:905
#120 0x5608a7a497c2 in erase<mojo::ServiceFactory::InstanceHolderBase*> J.J.J./base/containers/flat_tree.h:897
#121 0x5608a7a497c2 in ?? ???
#122 0x5608a7a494c2 in mojo::ServiceFactory::OnInstanceDisconnected(mojo::ServiceFactory::InstanceHolderBase*) J.J.J./mojo/public/cpp/bindings/service_factory.cc:49
#123 0x5608a7a494c2 in ?? ???
#124 0x5608a7a4a69d in base::internal::Invoker<base::internal::BindState<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase*),
base::WeakPtr<mojo::ServiceFactory>, mojo::ServiceFactory::InstanceHolderBase>, void (>):RunOnce(base::internal::BindStateBase*)> J.J.J./base/bind_internal.h:498
#125 0x5608a7a4a69d in MakeltSo<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase*), base::WeakPtr<mojo::ServiceFactory>,
mojo::ServiceFactory::InstanceHolderBase*> J.J.J./base/bind_internal.h:657
#126 0x5608a7a4a69d in RunImpl<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase*), std::tuple<base::WeakPtr<mojo::ServiceFactory>,
mojo::ServiceFactory::InstanceHolderBase*>, 0, 1> J.J.J./base/bind_internal.h:710
#127 0x5608a7a4a69d in RunOnce J.J.J./base/bind_internal.h:679
#128 0x5608a7a4a69d in ?? ???
#129 0x5608a7a4a961 in base::internal::Invoker<base::internal::BindState<base::internal::ThenHelper<base::OnceCallback<void (>), base::OnceCallback<void (>), void,
0>(>):lambda(base::OnceCallback<void (>), base::OnceCallback<void (>)>#1, base::OnceCallback<void (>), base::OnceCallback<void (>)>, void
(>):RunOnce(base::internal::BindStateBase*)> J.J.J./base/callback.h:101
#130 0x5608a7a4a961 in operator() J.J.J./base/callback_internal.h:210
#131 0x5608a7a4a961 in Invoke<lambda at J.J.J./base/callback_internal.h:209:10, base::OnceCallback<void (>), base::OnceCallback<void (>)> >
J.J.J./base/bind_internal.h:379
#132 0x5608a7a4a961 in MakeltSo<lambda at J.J.J./base/callback_internal.h:209:10, base::OnceCallback<void (>), base::OnceCallback<void (>)> >
J.J.J./base/bind_internal.h:637
#133 0x5608a7a4a961 in RunImpl<lambda at J.J.J./base/callback_internal.h:209:10, std::tuple<base::OnceCallback<void (>), base::OnceCallback<void (>)>, 0, 1>
J.J.J./base/bind_internal.h:710
#134 0x5608a7a4a961 in RunOnce J.J.J./base/bind_internal.h:679
#135 0x5608a7a4a961 in ?? ???
#136 0x5608a7a49d28 in mojo::ServiceFactory::InstanceHolderBase::OnPipeSignaled(unsigned int, mojo::HandleSignalsState const&) J.J.J./base/callback.h:101
#137 0x5608a7a49d28 in OnPipeSignaled J.J.J./mojo/public/cpp/bindings/service_factory.cc:80
#138 0x5608a7a49d28 in ?? ???
#139 0x5608a7a7967a in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&) J.J.J./base/callback.h:168
#140 0x5608a7a7967a in OnHandleReady J.J.J./mojo/public/cpp/system/simple_watcher.cc:278
#141 0x5608a7a7967a in ?? ???
#142 0x5608a7a7a8c3 in mojo::SimpleWatcher::Context::Notify(unsigned int, MojoHandleSignalsState, unsigned int) J.J.J./mojo/public/cpp/system/simple_watcher.cc:94
#143 0x5608a7a7a8c3 in ?? ???
#144 0x5608a7a776fa in mojo::SimpleWatcher::Context::CallNotify(MojoTrapEvent const*) J.J.J./mojo/public/cpp/system/simple_watcher.cc:59
#145 0x5608a7a776fa in ?? ???
#146 0x56089e324625 in mojo::core::WatcherDispatcher::InvokeWatchCallback(unsigned long, unsigned int, mojo::core::HandleSignalsState const&, unsigned int)
J.J.J./mojo/core/watcher_dispatcher.cc:94
#147 0x56089e324625 in ?? ???
#148 0x56089e3236aa in mojo::core::Watch::InvokeCallback(unsigned int, mojo::core::HandleSignalsState const&, unsigned int) J.J.J./mojo/core/watch.cc:78
#149 0x56089e3236aa in ?? ???
#150 0x56089e3176c8 in mojo::core::RequestContext::~RequestContext() J.J.J./mojo/core/request_context.cc:72
#151 0x56089e3176c8 in ?? ???
#152 0x56089e2f54db in mojo::core::NodeChannel::OnChannelError(mojo::core::Channel::Error) J.J.J./mojo/core/node_channel.cc:844
#153 0x56089e2f54db in ?? ???
#154 0x56089e337a22 in mojo::core::ChannelPosix::OnFileCanReadWithoutBlocking(int) J.J.J./mojo/core/channel_posix.cc:?
#155 0x56089e337a22 in ?? ???
#156 0x5608a612e94f in base::MessagePumpLibevent::OnLibeventNotification(int, short, void*) J.J.J./base/message_loop/message_pump_libevent.cc:?
#157 0x5608a612e94f in ?? ???
#158 0x5608a64eaf8c in event_process_active J.J.J./base/third_party/libevent/event.c:381
#159 0x5608a64eaf8c in event_base_loop J.J.J./base/third_party/libevent/event.c:521
#160 0x5608a64eaf8c in ?? ???
#161 0x5608a612f547 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) J.J.J./base/message_loop/message_pump_libevent.cc:260
#162 0x5608a612f547 in ?? ???
#163 0x5608a600c25c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
J.J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460
#164 0x5608a600c25c in ?? ???
#165 0x5608a5f54f41 in base::RunLoop::Run(base::Location const&) J.J.J./base/run_loop.cc:133
#166 0x5608a5f54f41 in ?? ???
#167 0x5608a60619a2 in base::Thread::Run(base::RunLoop*) J.J.J./base/threading/thread.cc:311
#168 0x5608a60619a2 in ?? ???
#169 0x5608a6061f13 in base::Thread::ThreadMain() J.J.J./base/threading/thread.cc:382
#170 0x5608a6061f13 in ?? ???
#171 0x5608a60ee945 in base::(anonymous namespace)::ThreadFunc(void*) J.J.J./base/threading/platform_thread_posix.cc:87
#172 0x5608a60ee945 in ?? ???
error: unknown argument '-demangle=True'
#173 0x7fae86812608 in start_thread /build/glibc-ZN95T4/glibc-2.31/nptl/ptthread_create.c:477
#174 0x7fae86812608 in ?? ???
```

```
0x60400004f22c is located 28 bytes inside of 40-byte region [0x60400004f210,0x60400004f238)
freed by thread T3 (Chrome_ChildIOT) here:
#0 0x560899a48d4d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160
#1 0x560899a48d4d in ?? ???
#2 0x5608abd2a115 in network::NetworkContext::~NetworkContext() J.J.J./buildtools/third_party/libc++/trunk/include/__tree:1821
#3 0x5608abd2a115 in ~map J.J.J./buildtools/third_party/libc++/trunk/include/map:1090
#4 0x5608abd2a115 in ~NetworkContext J.J.J./services/network/network_context.cc:534
#5 0x5608abd2a115 in ?? ???
#6 0x5608abd2aa7d in network::NetworkContext::~NetworkContext() J.J.J./services/network/network_context.cc:492
#7 0x5608abd2aa7d in ?? ???
#8 0x5608abd0ff1d in operator() J.J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#9 0x5608abd0ff1d in reset J.J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#10 0x5608abd0ff1d in ~unique_ptr J.J.J./buildtools/third_party/libc++/trunk/include/memory:2587
```

```
#11 0x5608abd0ff1d in __destroy<std::unique_ptr<network::NetworkContext> > /J.J./buildtools/third_party/libc++/trunk/include/memory:1787
#12 0x5608abd0ff1d in destroy<std::unique_ptr<network::NetworkContext> > /J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#13 0x5608abd0ff1d in std::_1::__tree<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> >,
base::UniquePtrComparator, std::_1::allocator<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> > >
>::destroy(std::_1::__tree_node<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> >, void*>*)
/J.J./buildtools/third_party/libc++/trunk/include/_tree:1833
#14 0x5608abd0ff1d in ?? ???:0
#15 0x5608abd0fed1 in std::_1::__tree<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> >,
base::UniquePtrComparator, std::_1::allocator<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> > >
>::destroy(std::_1::__tree_node<std::_1::unique_ptr<network::NetworkContext, std::_1::default_delete<network::NetworkContext> >, void*>*)
/J.J./buildtools/third_party/libc++/trunk/include/_tree:1831
#16 0x5608abd0fed1 in ?? ???:0
#17 0x5608abd05ae1 in clear /J.J./buildtools/third_party/libc++/trunk/include/_tree:1870
#18 0x5608abd05ae1 in clear /J.J./buildtools/third_party/libc++/trunk/include/set:693
#19 0x5608abd05ae1 in DestroyNetworkContexts /J.J./services/network/network_service.cc:855
#20 0x5608abd05ae1 in ~NetworkService /J.J./services/network/network_service.cc:409
#21 0x5608abd05ae1 in ?? ???:0
#22 0x5608abd065ed in network::NetworkService::~NetworkService() /J.J./services/network/network_service.cc:402
#23 0x5608abd065ed in ?? ???:0
#24 0x5608a54590ee in operator() /J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#25 0x5608a54590ee in reset /J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#26 0x5608a54590ee in ~unique_ptr /J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#27 0x5608a54590ee in ~InstanceHolder /J.J./mojo/public/cpp/bindings/service_factory.h:127
#28 0x5608a54590ee in ~InstanceHolder /J.J./mojo/public/cpp/bindings/service_factory.h:127
#29 0x5608a54590ee in ?? ???:0
#30 0x5608a7a497c2 in operator() /J.J./buildtools/third_party/libc++/trunk/include/memory:2378
#31 0x5608a7a497c2 in reset /J.J./buildtools/third_party/libc++/trunk/include/memory:2633
#32 0x5608a7a497c2 in ~unique_ptr /J.J./buildtools/third_party/libc++/trunk/include/memory:2587
#33 0x5608a7a497c2 in destroy /J.J./buildtools/third_party/libc++/trunk/include/memory:1920
#34 0x5608a7a497c2 in __destroy<std::unique_ptr<mojo::ServiceFactory::InstanceHolderBase> > /J.J./buildtools/third_party/libc++/trunk/include/memory:1782
#35 0x5608a7a497c2 in destroy<std::unique_ptr<mojo::ServiceFactory::InstanceHolderBase> > /J.J./buildtools/third_party/libc++/trunk/include/memory:1619
#36 0x5608a7a497c2 in __destruct_at_end /J.J./buildtools/third_party/libc++/trunk/include/vector:426
#37 0x5608a7a497c2 in __destruct_at_end /J.J./buildtools/third_party/libc++/trunk/include/vector:833
#38 0x5608a7a497c2 in erase /J.J./buildtools/third_party/libc++/trunk/include/vector:1738
#39 0x5608a7a497c2 in erase /J.J./base/containers/flat_tree.h:905
#40 0x5608a7a497c2 in erase<mojo::ServiceFactory::InstanceHolderBase *> /J.J./base/containers/flat_tree.h:897
#41 0x5608a7a497c2 in ?? ???:0
#42 0x5608a7a494c2 in mojo::ServiceFactory::OnInstanceDisconnected(mojo::ServiceFactory::InstanceHolderBase*) /J.J./mojo/public/cpp/bindings/service_factory.cc:49
#43 0x5608a7a494c2 in ?? ???:0
#44 0x5608a7a4a69d in Invoke<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase *), base::WeakPtr<mojo::ServiceFactory>,
mojo::ServiceFactory::InstanceHolderBase *> /J.J./base/bind_internal.h:498
#45 0x5608a7a4a69d in MakeltSo<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase *), base::WeakPtr<mojo::ServiceFactory>,
mojo::ServiceFactory::InstanceHolderBase *> /J.J./base/bind_internal.h:657
#46 0x5608a7a4a69d in RunImpl<void (mojo::ServiceFactory::*)(mojo::ServiceFactory::InstanceHolderBase *), std::tuple<base::WeakPtr<mojo::ServiceFactory>,
mojo::ServiceFactory::InstanceHolderBase *>, 0, 1> /J.J./base/bind_internal.h:710
#47 0x5608a7a4a69d in RunOnce /J.J./base/bind_internal.h:679
#48 0x5608a7a4a69d in ?? ???:0
#49 0x5608a7a4a961 in Run /J.J./base/callback.h:101
#50 0x5608a7a4a961 in operator() /J.J./base/callback_internal.h:210
#51 0x5608a7a4a961 in Invoke<(lambda at /J.J./base/callback_internal.h:209:10), base::OnceCallback<void ()>, base::OnceCallback<void ()> >
/J.J./base/bind_internal.h:379
#52 0x5608a7a4a961 in MakeltSo<(lambda at /J.J./base/callback_internal.h:209:10), base::OnceCallback<void ()>, base::OnceCallback<void ()> >
/J.J./base/bind_internal.h:637
#53 0x5608a7a4a961 in RunImpl<(lambda at /J.J./base/callback_internal.h:209:10), std::tuple<base::OnceCallback<void ()>, base::OnceCallback<void ()> >, 0, 1>
/J.J./base/bind_internal.h:710
#54 0x5608a7a4a961 in RunOnce /J.J./base/bind_internal.h:679
#55 0x5608a7a4a961 in ?? ???:0
#56 0x5608a7a49d28 in Run /J.J./base/callback.h:101
#57 0x5608a7a49d28 in OnPipeSignaled /J.J./mojo/public/cpp/bindings/service_factory.cc:80
#58 0x5608a7a49d28 in ?? ???:0
#59 0x5608a7a7967a in Run /J.J./base/callback.h:168
#60 0x5608a7a7967a in OnHandleReady /J.J./mojo/public/cpp/system/simple_watcher.cc:278
#61 0x5608a7a7967a in ?? ???:0
#62 0x5608a7a7a8c3 in mojo::SimpleWatcher::Context::Notify(unsigned int, MojoHandleSignalsState, unsigned int) /J.J./mojo/public/cpp/system/simple_watcher.cc:94
#63 0x5608a7a7a8c3 in ?? ???:0
#64 0x5608a7a776fa in mojo::SimpleWatcher::Context::CallNotify(MojoTrapEvent const*) /J.J./mojo/public/cpp/system/simple_watcher.cc:59
#65 0x5608a7a776fa in ?? ???:0
#66 0x56089e324625 in mojo::core::WatcherDispatcher::InvokeWatchCallback(unsigned long, unsigned int, mojo::core::HandleSignalsState const&, unsigned int)
/J.J./mojo/core/watcher_dispatcher.cc:94
#67 0x56089e324625 in ?? ???:0
#68 0x56089e3236aa in mojo::core::Watch::InvokeCallback(unsigned int, mojo::core::HandleSignalsState const&, unsigned int) /J.J./mojo/core/watch.cc:78
#69 0x56089e3236aa in ?? ???:0
#70 0x56089e3176c8 in mojo::core::RequestContext::~RequestContext() /J.J./mojo/core/request_context.cc:72
#71 0x56089e3176c8 in ?? ???:0
#72 0x56089e2f54db in mojo::core::NodeChannel::OnChannelError(mojo::core::Channel::Error) /J.J./mojo/core/node_channel.cc:844
#73 0x56089e2f54db in ?? ???:0
#74 0x56089e337a22 in mojo::core::ChannelPosix::OnFileCanReadWithoutBlocking(int) channel_posix.cc:?
#75 0x56089e337a22 in ?? ???:0
#76 0x5608a612e94f in base::MessagePumpLibevent::OnLibeventNotification(int, short, void*) message_pump_libevent.cc:?
#77 0x5608a612e94f in ?? ???:0
#78 0x5608a64eaf8c in event_process_active /J.J./base/third_party/libevent/event.c:381
#79 0x5608a64eaf8c in event_base_loop /J.J./base/third_party/libevent/event.c:521
#80 0x5608a64eaf8c in ?? ???:0
#81 0x5608a612f547 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) /J.J./base/message_loop/message_pump_libevent.cc:260
#82 0x5608a612f547 in ?? ???:0
#83 0x5608a600c25c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
/J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460
#84 0x5608a600c25c in ?? ???:0
#85 0x5608a5f54f41 in base::RunLoop::Run(base::Location const&) /J.J./base/run_loop.cc:133
#86 0x5608a5f54f41 in ?? ???:0
#87 0x5608a60619a2 in base::Thread::Run(base::RunLoop*) /J.J./base/threading/thread.cc:311
#88 0x5608a60619a2 in ?? ???:0
#89 0x5608a6061f13 in base::Thread::ThreadMain() /J.J./base/threading/thread.cc:382
#90 0x5608a6061f13 in ?? ???:0
#91 0x5608a60ee945 in base::(anonymous namespace)::ThreadFunc(void*) /J.J./base/threading/platform_thread_posix.cc:87
#92 0x5608a60ee945 in ?? ???:0
#93 0x7fae86812608 in start_thread /build/glibc-ZN95T4/glibc-2.31/nptl pthread_create.c:477
#94 0x7fae86812608 in ?? ???:0
```

previously allocated by thread T3 (Chrome_ChildIOT) here:

```
#0 0x560899a484ed in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99
#1 0x560899a484ed in ?? ???:0
#2 0x5608abd2db8e in network::NetworkContext::LoaderCreated(unsigned int) /J.J./buildtools/third_party/libc++/trunk/include/new:253
```

```

#3 0x5608abd2db8e in allocate J.J.J./buildtools/third_party/libc++/trunk/include/memory:1853
#4 0x5608abd2db8e in allocate J.J.J./buildtools/third_party/libc++/trunk/include/memory:1570
#5 0x5608abd2db8e in __construct_node<const std::piecewise_construct_t &, std::tuple<const unsigned int &,>, std::tuple<>> >
J.J.J./buildtools/third_party/libc++/trunk/include/_tree:2190
#6 0x5608abd2db8e in __emplace_unique_key_args<unsigned int, const std::piecewise_construct_t &, std::tuple<const unsigned int &,>, std::tuple<>> >
J.J.J./buildtools/third_party/libc++/trunk/include/_tree:2136
#7 0x5608abd2db8e in operator[] J.J.J./buildtools/third_party/libc++/trunk/include/map:1519
#8 0x5608abd2db8e in LoaderCreated J.J.J./services/network/network_context.cc:706
#9 0x5608abd2db8e in ?? ???:0
#10 0x5608abe157a4 in network::cors::CorsURLLoaderFactory::OnLoaderCreated(std::::__1::unique_ptr<network::mojom::URLLoader,
std::::__1::default_delete<network::mojom::URLLoader>>) J.J.J./services/network/cors/cors_url_loader_factory.cc:227
#11 0x5608abe157a4 in ?? ???:0
#12 0x5608abf1c1d3 in network::URLLoaderFactory::CreateLoaderAndStart(mojom::PendingReceiver<network::mojom::URLLoader>, int, int, unsigned int,
network::ResourceRequest const&, mojom::PendingRemote<network::mojom::URLLoaderClient>, net::MutableNetworkTrafficAnnotationTag const&)
J.J.J./services/network/url_loader_factory.cc:299
#13 0x5608abf1c1d3 in ?? ???:0
#14 0x5608abe160e5 in network::cors::CorsURLLoaderFactory::CreateLoaderAndStart(mojom::PendingReceiver<network::mojom::URLLoader>, int, int, unsigned int,
network::ResourceRequest const&, mojom::PendingRemote<network::mojom::URLLoaderClient>, net::MutableNetworkTrafficAnnotationTag const&)
J.J.J./services/network/cors/cors_url_loader_factory.cc:277
#15 0x5608abe160e5 in ?? ???:0
#16 0x56089b571901 in network::mojom::URLLoaderFactoryStubDispatch::Accept(network::mojom::URLLoaderFactory*, mojom::Message*)
Jgen/services/network/public/mojom/url_loader_factory.mojom.cc:234
#17 0x56089b571901 in ?? ???:0
#18 0x5608a7a183f6 in mojom::InterfaceEndpointClient::HandleValidatedMessage(mojom::Message*) J.J.J./mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:554
#19 0x5608a7a183f6 in ?? ???:0
#20 0x5608a7a2517c in mojom::MessageDispatcher::Accept(mojom::Message*) J.J.J./mojo/public/cpp/bindings/lib/message_dispatcher.cc:46
#21 0x5608a7a2517c in ?? ???:0
#22 0x5608a7a30d7c in mojom::internal::MultiplexRouter::ProcessIncomingMessage(mojom::internal::MultiplexRouter::MessageWrapper*,
mojom::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*) J.J.J./mojo/public/cpp/bindings/lib/multiplex_router.cc:955
#23 0x5608a7a30d7c in ?? ???:0
#24 0x5608a7a24b8 in mojom::internal::MultiplexRouter::Accept(mojom::Message*) J.J.J./mojo/public/cpp/bindings/lib/multiplex_router.cc:622
#25 0x5608a7a24b8 in ?? ???:0
#26 0x5608a7a25266 in mojom::MessageDispatcher::Accept(mojom::Message*) J.J.J./mojo/public/cpp/bindings/lib/message_dispatcher.cc:41
#27 0x5608a7a25266 in ?? ???:0
#28 0x5608a7a117c3 in mojom::Connector::DispatchMessage(mojom::Message) J.J.J./mojo/public/cpp/bindings/lib/connector.cc:508
#29 0x5608a7a117c3 in ?? ???:0
#30 0x5608a7a13570 in mojom::Connector::ReadAllAvailableMessages() J.J.J./mojo/public/cpp/bindings/lib/connector.cc:566
#31 0x5608a7a13570 in ?? ???:0
#32 0x5608a7a7967a in Run J.J.J./base/callback.h:168
#33 0x5608a7a7967a in OnHandleReady J.J.J./mojo/public/cpp/system/simple_watcher.cc:278
#34 0x5608a7a7967a in ?? ???:0
#35 0x5608a7a7a8c3 in mojom::SimpleWatcher::Context::Notify(unsigned int, MojoHandleSignalsState, unsigned int) J.J.J./mojo/public/cpp/system/simple_watcher.cc:94
#36 0x5608a7a7a8c3 in ?? ???:0
#37 0x5608a7a776fa in mojom::SimpleWatcher::Context::CallNotify(MojoTrapEvent const*) J.J.J./mojo/public/cpp/system/simple_watcher.cc:59
#38 0x5608a7a776fa in ?? ???:0
#39 0x56089e324625 in mojom::core::WatcherDispatcher::InvokeWatchCallback(unsigned long, unsigned int, mojom::core::HandleSignalsState const&, unsigned int)
J.J.J./mojo/core/watcher_dispatcher.cc:94
#40 0x56089e324625 in ?? ???:0
#41 0x56089e3236aa in mojom::core::Watch::InvokeCallback(unsigned int, mojom::core::HandleSignalsState const&, unsigned int) J.J.J./mojo/core/watch.cc:78
#42 0x56089e3236aa in ?? ???:0
#43 0x56089e3176c8 in mojom::core::RequestContext::~RequestContext() J.J.J./mojo/core/request_context.cc:72
#44 0x56089e3176c8 in ?? ???:0
#45 0x56089e2f4472 in mojom::core::NodeChannel::OnChannelMessage(void const*, unsigned long, std::::__1::vector<mojom::PlatformHandle,
std::::__1::allocator<mojom::PlatformHandle>>) J.J.J./mojo/core/node_channel.cc:825
#46 0x56089e2f4472 in ?? ???:0
#47 0x56089e2c3863 in mojom::core::Channel::TryDispatchMessage(base::span<char const, 18446744073709551615ul>, unsigned long*) J.J.J./mojo/core/channel.cc:710
#48 0x56089e2c3863 in ?? ???:0
#49 0x56089e2c2f72 in mojom::core::Channel::OnReadComplete(unsigned long, unsigned long*) J.J.J./mojo/core/channel.cc:610
#50 0x56089e2c2f72 in ?? ???:0
#51 0x56089e337725 in mojom::core::ChannelPosix::OnFileCanReadWithoutBlocking(int) J.J.J./mojo/core/channel_posix.cc:318
#52 0x56089e337725 in ?? ???:0
#53 0x5608a612e94f in base::MessagePumpLibevent::OnLibeventNotification(int, short, void*) message_pump_libevent.cc:?
#54 0x5608a612e94f in ?? ???:0
#55 0x5608a64eaf8c in event_process_active J.J.J./base/third_party/libevent/event.c:381
#56 0x5608a64eaf8c in event_base_loop J.J.J./base/third_party/libevent/event.c:521
#57 0x5608a64eaf8c in ?? ???:0
#58 0x5608a612f547 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) J.J.J./base/message_loop/message_pump_libevent.cc:260
#59 0x5608a612f547 in ?? ???:0
#60 0x5608a600c25c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
J.J.J./base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460
#61 0x5608a600c25c in ?? ???:0
#62 0x5608a5f54f41 in base::RunLoop::Run(base::Location const&) J.J.J./base/run_loop.cc:133
#63 0x5608a5f54f41 in ?? ???:0
#64 0x5608a60619a2 in base::Thread::Run(base::RunLoop*) J.J.J./base/threading/thread.cc:311
#65 0x5608a60619a2 in ?? ???:0
#66 0x5608a6061f13 in base::Thread::ThreadMain() J.J.J./base/threading/thread.cc:382
#67 0x5608a6061f13 in ?? ???:0

```

Thread T3 (Chrome_ChildIOT) created by T0 (chrome) here:

```

#0 0x560899a07e4a in __interceptor_pthread_create /b/s/w/ir/cache/builder/src/third_party/lvm/compiler-rt/lib/asan/asan_interceptors.cpp:214
#1 0x560899a07e4a in ?? ???:0
#2 0x5608a60edbce in base::(anonymous namespace)::CreateThread(unsigned long, bool, base::PlatformThread::Delegate*, base::PlatformThreadHandle*,
base::ThreadPriority) J.J.J./base/threading/platform_thread_posix.cc:126
#3 0x5608a60edbce in ?? ???:0
#4 0x5608a6060cfd in base::Thread::StartWithOptions(base::Thread::Options const&) J.J.J./base/threading/thread.cc:186
#5 0x5608a6060cfd in ?? ???:0
#6 0x5608b2b36239 in content::ChildProcess::ChildProcess(base::ThreadPriority, std::::__1::basic_string<char, std::::__1::char_traits<char>, std::::__1::allocator<char>>
const&, std::::__1::unique_ptr<base::ThreadPoolInstance::InitParams, std::::__1::default_delete<base::ThreadPoolInstance::InitParams>>)
J.J.J./content/child/child_process.cc:111
#7 0x5608b2b36239 in ?? ???:0
#8 0x5608a545d9b7 in content::UtilityMain(content::MainFunctionParams const&) J.J.J./content/utility/utility_main.cc:127
#9 0x5608a545d9b7 in ?? ???:0
#10 0x5608a5cb0fed in content::ContentMainRunnerImpl::Run(bool) J.J.J./content/app/content_main_runner_impl.cc:877
#11 0x5608a5cb0fed in ?? ???:0
#12 0x5608a5caad36 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) J.J.J./content/app/content_main.cc:372
#13 0x5608a5caad36 in ?? ???:0
#14 0x5608a5cab33c in content::ContentMain(content::ContentMainParams const&) J.J.J./content/app/content_main.cc:398
#15 0x5608a5cab33c in ?? ???:0
#16 0x560899a4b007 in ChromeMain J.J.J./chrome/app/chrome_main.cc:141

```

Did this work before? N/A

Chrome version: 89.0.4350.4 Channel: n/a

OS Version: 20.04

Flash Version:

crash.html

357 bytes [View](#) [Download](#)

[Comment 1](#) by [sheriffbot](#) on Fri, Feb 5, 2021, 1:54 AM EST Project Member

Labels: external_security_report

[Comment 2](#) by [tsepez@chromium.org](#) on Fri, Feb 5, 2021, 1:40 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: lukasza@chromium.org

Labels: Security_Severity-Medium Security_Impact-Stable

Components: Internals>Network

lukasza - looks like you've investigated some crashes in the code in the past, could you kindly take a look or re-assign as appropriate? Thanks!
Setting to sev-medium as interaction required seems to involve interrupting a shutdown that was previously interrupted.

[Comment 3](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:02 PM EST Project Member

Free - casuation chain / reversed ~callstack:

```
1. void ServiceFactory::OnInstanceDisconnected(InstanceHolderBase* instance) {
    instances_.erase(instance);
}
1b. ~InstanceHolder

2. NetworkService::~NetworkService() {
    DCHECK_EQ(this, g_network_service);
    ...
    g_network_service = nullptr;
    ...
    DestroyNetworkContexts();
    ...

3. ~NetworkContext
~map (hypothesis - this corresponds to the map in
    NetworkContext::loader_count_per_process_)
```

Use-after-free - casuation chain / reversed ~callstack:

```
1. network::URLLoader::OnResponseStarted
1b. network::URLLoader::DeleteSelf

2. void CorsURLLoaderFactory::DestroyURLLoader(mojom::URLLoader* loader) {
    if (context_)
        context_>LoaderDestroyed(process_id_);
    ...

3. void NetworkContext::LoaderDestroyed(uint32_t process_id) {
    // [this] has been freed already.
    // Same for |loader_count_per_process_|.
    auto it = loader_count_per_process_.find(process_id);
    ...
```

I also observe that NetworkContext owns the CorsURLLoaderFactory and the |loader_count_per_process_|, but the factory is destroyed "later" than |loader_count_per_process_| (this order seems wrong):

```
// This must be below |url_request_context_| so that the URLRequestContext
// outlives all the URLLoaderFactories and URLLoaders that depend on it;
// for the same reason, it must also be below |network_context_|.
std::set<std::unique_ptr<CorsURLLoaderFactory>,
    base::UniquePtrComparator>
url_loader_factories_;
...
// A count of outstanding requests per initiating process.
std::map<uint32_t, uint32_t> loader_count_per_process_;
```

So, I guess a tentative/speculative fix would be to move the declaration of the `url_loader_factories_` field further down.

[Comment 4](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:07 PM EST Project Member

+mmenke@, since he tweaked the order of field declarations (i.e. moved `url_loader_factories_` in [r548193](#))

[Comment 5](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:09 PM EST Project Member

Cc: mmenke@chromium.org

[Comment 6](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:17 PM EST Project Member

FWIW, I've put together a WIP CL with the fix idea based on [#c3](#) - see: <https://crrev.com/c/2679230>

Services_unittests + navigational content_browserests are passing on my machine - let's see what CQ says though...

I am not very familiar with the multitude of NetworkContext's fields, but so far I didn't see any fields that obviously should be destroyed "before" `url_loader_factories_`. Ultimately though, I would rely on a code review from //services/network/OWNERS (mmenke@? :-).

[Comment 7](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:21 PM EST Project Member

tsepez@ (or other security sheriffs) - what level of verification should I do for the speculative fix from [#c6](#)?

1. Can I just land it and hope that it fixes the issue (and/or that somebody else can verify that it fixed the issue)?

vs

2. Should I attempt to repro the UaF locally and make sure that it goes away after the fix? How safe is it to navigate to the PoC (e.g. crash.html + [https://fonts.gstatic.com/s/bitter/v7/HEpP8tXlWwYHimsnXg\(COvvDin1pK8aKteLpeZ5c0A.woff2\)](https://fonts.gstatic.com/s/bitter/v7/HEpP8tXlWwYHimsnXg(COvvDin1pK8aKteLpeZ5c0A.woff2)))? It is easiest for me to build Chrome with the fix locally, on my primary dev machine, bit I guess I can provide Linux binaries to try on other machines (VMs?) if needed?

[Comment 8](#) by [lukasza@chromium.org](#) on Fri, Feb 5, 2021, 4:22 PM EST Project Member

tsepez@ (or other security sheriffs) - do we need to make sure (in this bug? in a follow-up?) that this kind of a scenario is covered by ClusterFuzz or other such testing infrastructure? Not sure how to do that myself... :-/

[Comment 9](#) by [sheriffbot](#) on Sat, Feb 6, 2021, 1:02 PM EST Project Member

Labels: Target-89 M-89

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

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

Comment 10 by [sheriffbot](#) on Sat, Feb 6, 2021, 1:38 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 11 by [bugdroid](#) on Tue, Feb 9, 2021, 2:50 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+f2b091f02593c67fd67db936452f363102b8d035>

commit [f2b091f02593c67fd67db936452f363102b8d035](#)

Author: Lukasz Anforowicz <lukasza@chromium.org>

Date: Tue Feb 09 19:50:37 2021

Destroy `url_loader_factories_` before other NetworkContext fields.

[Bug-1174043](#)

Change-Id: I7488c7779f51a3f0d82ecad3d65446032c065b26

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2679230>

Commit-Queue: Lukasz Anforowicz <lukasza@chromium.org>

Reviewed-by: Matt Menke <mmenke@chromium.org>

Cr-Commit-Position: refs/heads/master@{#852311}

[modify] https://crrev.com/f2b091f02593c67fd67db936452f363102b8d035/services/network/network_context.h

Comment 12 by lukasza@chromium.org on Tue, Feb 9, 2021, 3:03 PM EST Project Member

Let's wait until the fix in [r852311](#) above is included in a Canary release (maybe in 90.0.4414.x tomorrow?) and then we can try to verify the fix (hopefully with assistance from emilykim8708@).

Comment 13 by emily...@gmail.com on Tue, Feb 9, 2021, 8:18 PM EST

I've tested it many times(Chromium 89.0.4350.4 with above patch) and can't reproduce the crash again.

Comment 14 by rsesek@chromium.org on Wed, Feb 10, 2021, 4:58 PM EST Project Member

[Issue-1176644](#) has been merged into this issue.

Comment 15 by [ClusterFuzz](#) on Wed, Feb 10, 2021, 5:03 PM EST Project Member

Labels: Unreproducible

ClusterFuzz testcase 5317650078302208 appears to be flaky, updating reproducibility label.

Comment 16 by lukasza@chromium.org on Wed, Feb 10, 2021, 5:09 PM EST Project Member

Status: Fixed (was: Assigned)

RE: [#c13](#): emilykim8708@:

89.0.4350.4 doesn't contain the patch above - commit [f2b091f0...](#) initially landed in 90.0.4414.0.

I guess I could ask you to verify on 90.0.4414.0, but I am not sure how much we should collectively trust such verification given that even without the fix the issue seems difficult to repro (per [#c13](#) above + per ClusterFuzz report in [issue-1176644](#)).

Still, based on the bug report + reading the code, I think that [r852311](#) should be the right fix, so let me mark the bug as fixed.

Comment 17 by lukasza@chromium.org on Wed, Feb 10, 2021, 5:18 PM EST Project Member

Cc: pbomm...@chromium.org benmason@chromium.org

Labels: Merge-Request-89

+pbommana@ (the M89 TPM for desktop) - PTAL at the merge request?

[AFAIK this bug affects all NetworkService platforms, but I wasn't sure if I should be CC-ing/spamming Android and CrOS TPMs :-)]

Adding the Merge-Request-89 label for [r852311](#), because:

1. the merge seems desirable:

- 1.1. this bug is already labelled with Target-89
- 1.2. this is a medium severity security bug

2. the merge seems safe:

- 2.1. the fix in [r852311](#) is relatively simple and low-risk
- 2.2. we are still ~3 weeks away from M89 Stable Release
- 2.3. the fix has started baking in the Canary channel in 90.0.4414.0

Comment 18 by [sheriffbot](#) on Wed, Feb 10, 2021, 5:23 PM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:

8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: <http://go/cros-engprodcomponents>

Please contact the milestone owner if you have questions.

Owners: benmason@(Android), bindusuvama@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 19 by lukasza@chromium.org on Wed, Feb 10, 2021, 5:55 PM EST Project Member

RE: 1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: <https://goto.google.com/cros-release-branch-merge-guidelines>

I believe so. We are in "phase 3 / last two weeks of Beta" of M89. This is a medium-severity security bug.

RE: 2. Links to the CLs you are requesting to merge.

[r852311](#)

RE: 3. Has the change landed and been verified on ToT?

The change has landed in 90.0.4414.0. There are no known adverse effects from the change (crash reports, pinpoint problems, etc). OTOH, the problem involved a race and therefore the change is tricky to verify (see [#c16](#)).

RE: 4. Does this change need to be merged into other active release branches (M-1, M+1)?

I don't know. I'll let LTS team make that judgement. I trust that they are monitoring security bugs.

RE: 5. Why are these changes required in this milestone after branch?

The security bug has not been detected until recently.

RE: 6. Is this a new feature?

No.

RE: 7. If it is a new feature, is it behind a flag using finch?

N/A

[Comment 20](#) by [sheriffbot](#) on Thu, Feb 11, 2021, 12:43 PM EST Project Member
Labels: reward-topanel

[Comment 21](#) by [sheriffbot](#) on Thu, Feb 11, 2021, 1:58 PM EST Project Member
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

[Comment 22](#) by [adetaylor@google.com](#) on Fri, Feb 12, 2021, 1:36 PM EST Project Member
Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389, assuming it's still the case that no problems have shown up in Canary.

[Comment 23](#) by [bugdroid](#) on Fri, Feb 12, 2021, 3:47 PM EST Project Member
Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+ffeb0731f83f8c4fa72776b658df45f0e6da041c>

commit [ffeb0731f83f8c4fa72776b658df45f0e6da041c](#)
Author: Lukasz Anforowicz <lukasza@chromium.org>
Date: Fri Feb 12 20:45:21 2021

M89: Destroy `url_loader_factories_` before other NetworkContext fields

(cherry picked from commit [f2b091f02593c67fd67db936452f363102b8d035](#))

~~[Bug-1474049](#)~~

Change-Id: I7488c7779f51a3f0d82ecad3d65446032c065b26
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2679230>
Commit-Queue: Lukasz Anforowicz <lukasza@chromium.org>
Reviewed-by: Matt Menke <mmenke@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#852311}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2692489>
Reviewed-by: Lukasz Anforowicz <lukasza@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4389@{#986}
Cr-Branched-From: [9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7](#)-refs/heads/master@{#843830}

[modify] https://crrev.com/ffeb0731f83f8c4fa72776b658df45f0e6da041c/services/network/network_context.h

[Comment 24](#) by [adetaylor@google.com](#) on Fri, Feb 26, 2021, 1:08 PM EST Project Member
Labels: Release-0-M89

[Comment 25](#) by [adetaylor@google.com](#) on Mon, Mar 1, 2021, 7:28 PM EST Project Member
Labels: CVE-2021-21179 CVE_description-missing

[Comment 26](#) by [vsavu@google.com](#) on Wed, Mar 3, 2021, 5:06 AM EST Project Member
Labels: LTS-Merge-Request-86

[Comment 27](#) by [vsavu@google.com](#) on Wed, Mar 3, 2021, 5:59 AM EST Project Member
Labels: LTS-Security-86

[Comment 28](#) by [gianluca@google.com](#) on Wed, Mar 3, 2021, 10:33 AM EST Project Member
Labels: LTS-Merge-Approved-86

[Comment 29](#) by [Git Watcher](#) on Thu, Mar 4, 2021, 12:08 PM EST Project Member
Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+c6d6f7aee733b2a21378e3d1b2990b50d68eb457>

commit [c6d6f7aee733b2a21378e3d1b2990b50d68eb457](#)
Author: Lukasz Anforowicz <lukasza@chromium.org>
Date: Thu Mar 04 17:07:16 2021

M86-LTS: Destroy `url_loader_factories_` before other NetworkContext fields

[M86 Merge]: Fixed conflict in network_context.h.

(cherry picked from commit [f2b091f02593c67fd67db936452f363102b8d035](#))

(cherry picked from commit [fdeb0731f83f8c4fa72776b658df45f0e6da041c](#))

[Bug=4474943](#)

Change-Id: I7488c7779f51a3f0d82ecad3d65446032c065b26

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2679230>

Commit-Queue: Łukasz Anforowicz <lukasza@chromium.org>

Reviewed-by: Matt Menke <mmenke@chromium.org>

Cr-Original-Original-Commit-Position: refs/heads/master@{#852311}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2692489>

Reviewed-by: Łukasz Anforowicz <lukasza@chromium.org>

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Cr-Original-Commit-Position: refs/branch-heads/4389@{#986}

Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2731372>

Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>

Reviewed-by: Achuth Bhandarkar <achuith@chromium.org>

Cr-Commit-Position: refs/branch-heads/4240@{#1559}

Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/c6d6f7aee733b2a21378e3d1b2990b50d68eb457/services/network/network_context.h

Comment 30 by vsavu@google.com on Mon, Mar 8, 2021, 11:16 AM EST Project Member

Labels: -LTS-Merge-Approved-86 -LTS-Merge-Request-86 LTR-Merged-86

Comment 31 by amyressler@google.com on Tue, Mar 9, 2021, 12:59 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by amyressler@google.com on Wed, Mar 10, 2021, 6:30 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-15000

*** 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 33 by amyressler@google.com on Wed, Mar 10, 2021, 6:59 PM EST Project Member

Congratulations, emilykim@! The VRP Panel has decided to award you \$15,000 for this report. Thanks for your effort and great work!

Comment 34 by amyressler@google.com on Thu, Mar 11, 2021, 12:48 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 35 by [sheriffbot](#) on Fri, Jun 11, 2021, 1:51 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