Starred by 3 users

Owner: jarrydg@chromium.org
Last visit 19 days ago

CC: pbommana@google.com
gov...@chromium.org
benmason@chromium.org
jsb...@chromium.org
pbomm...@chromium.org
mek@chromium.org
dmu...@chromium.org
pwnall@chromium.org
amyressler@chromium.org
marinakz@chromium.org
nasko@chromium.org

Status: Fixed *(Closed)*

Components: Blink>Storage

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros

Pri: 0

Type: Bug-Security

Hotlist-Merge-Review
Stability-Memory-AddressSanitizer
Security_Severity-Critical
Arch-x86_64
Hotlist-Merge-Approved
allpublic
reward-inprocess
Unreproducible
Via-Wizard-Security
reward-20000
Test-Predator-Auto-Components
CVE_description-submitted
external_security_report
M-96
Target-96

FoundIn-96
Security_Impact-Extended
merge-merged-4664

Issue 1275020: SUMMARY: AddressSanitizer: heap-use-after-free base/bind_internal.h:535:12 in BindState<void (content::StorageNotificationService::*)(url::Origin), UnretainedWrapper<content::StorageNotificationService>

Reported by m.coo...@gmail.com on Tue, Nov 30, 2021, 3:42 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4676.0 Safari/537.36

Steps to reproduce the problem:
#TestOn
asan-linux-release-945738

#Reproduce
This is found by my fuzzer running on ClusterFuzz, but it cannot be reproduced stably so ClusterFuzz does not automatically open a case.
https://clusterfuzz.com/testcase-detail/6255222588243968 (may require the security team to set permissions)

What is the expected behavior?

What went wrong?
Type of crash
browser process(may cause the sandbox escape)

#Analysis

1. StoragePartitionImpl::Initialize call GetStorageNotificationService get a raw pointer of StorageNotificationService and call BindRepeating make a RepeatingCallback pass as paramer of SetStoragePressureCallback(See the asan log alloc stack for details)
2. When KeyedServiceFactory::Disassociate is called, it will delete all members of mapping_(See the asan log free stack for details), which will cause SetStoragePressureCallback to retain a wild pointer of StorageNotificationService
3. When the callback condition of SetStoragePressureCallback is met, the previously generated RepeatingCallback is called, resulting in UAF.

```
//content/browser/storage_partition_impl.cc:1186
void StoragePartitionImpl::Initialize(
    StoragePartitionImpl* fallback_for_blob_urls) {
  // Ensure that these methods are called on the UI thread, except for
  // unittests where a UI thread might not have been created.
  DCHECK(BrowserThread::CurrentlyOn(BrowserThread::UI) ||
         !BrowserThread::IsThreadInitialized(BrowserThread::UI));
  DCHECK(!initialized_);
  initialized_ = true;
--CUT--

  StorageNotificationService* storage_notification_service =
      browser_context_->GetStorageNotificationService();
  if (storage_notification_service) {
```

```
   // base::Unretained is safe to use because the BrowserContext is guaranteed
   // to outlive QuotaManager. This is because BrowserContext outlives this
   // StoragePartitionImpl, which destroys the QuotaManager on teardown.
   base::RepeatingCallback<void(const blink::StorageKey)>
      send_notification_function = base::BindRepeating(
         [](StorageNotificationService* service,
            const blink::StorageKey storage_key) {
           GetUIThreadTaskRunner({})->PostTask(
              FROM_HERE,
              base::BindOnce(&StorageNotificationService::
                               MaybeShowStoragePressureNotification,
                             base::Unretained(service),
                             std::move(storage_key.origin())));
         },
         base::Unretained(storage_notification_service));              <<[1]

   quota_manager_->SetStoragePressureCallback(send_notification_function);  <<[1]
  }

components/keyed_service/core/keyed_service_factory.h:88
// The mapping between a context and its service.
std::map<void*, std::unique_ptr<KeyedService>> mapping_; <<[2]

//components/keyed_service/core/keyed_service_factory.cc:94
void KeyedServiceFactory::Disassociate(void* context) {
  auto iterator = mapping_.find(context);
  if (iterator != mapping_.end())
    mapping_.erase(iterator);           <<[3]
}
```

#Patch
Not yet

#asan
```
==================================================================
==329557==ERROR: AddressSanitizer: heap-use-after-free on address 0x604000685aa0 at pc 0x55b61cb418b8 bp
0x7fff5635b930 sp 0x7fff5635b928
READ of size 8 at 0x604000685aa0 thread T0 (chrome)
SCARINESS: 51 (8-byte-read-heap-use-after-free)
    #0 0x55b61cb418b7 in base::internal::Invoker<base::internal::BindState<void (content::StorageNotificationService::*)
(url::Origin), base::internal::UnretainedWrapper<content::StorageNotificationService>, url::Origin>, void
()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:535:12
    #1 0x55b624d9edc3 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/callback.h:142:12
    #2 0x55b624dd9773 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) base/task/common/task_annotator.h:74:5
    #3 0x55b624dd8f87 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #4 0x55b624dda341 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
    #5 0x55b624c953fa in base::MessagePumpGlib::Run(base::MessagePump::Delegate*)
```

base/message_loop/message_pump_glib.cc:405:48
    #6 0x55b624ddaa0b in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta) base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:468:12
    #7 0x55b624d171a9 in base::RunLoop::Run(base::Location const&) base/run_loop.cc:140:14
    #8 0x55b61ba2d0f8 in content::BrowserMainLoop::RunMainMessageLoop() content/browser/browser_main_loop.cc:1001:18
    #9 0x55b61ba319c5 in content::BrowserMainRunnerImpl::Run() content/browser/browser_main_runner_impl.cc:153:15
    #10 0x55b61ba27377 in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:30:28
    #11 0x55b623b6c8b0 in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:646:10
    #12 0x55b623b6f97a in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool) content/app/content_main_runner_impl.cc:1159:10
    #13 0x55b623b6ea52 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1026:12
    #14 0x55b623b675ec in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*) content/app/content_main.cc:398:36
    #15 0x55b623b69214 in content::ContentMain(content::ContentMainParams) content/app/content_main.cc:426:10
    #16 0x55b616b4e2de in ChromeMain chrome/app/chrome_main.cc:172:12
    #17 0x7f1f0c34482f in __libc_start_main /build/glibc-LK5gWL/glibc-2.23/csu/../csu/libc-start.c:291
0x604000685aa0 is located 0 bytes inside of 24-byte region [0x604000685aa0,0x604000685ab8)
freed by thread T0 (chrome) here:
    #0 0x55b616b4c29d in operator delete(void*) third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:152:3
    #1 0x55b628e499eb in KeyedServiceFactory::Disassociate(void*) buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
    #2 0x55b628e49bc5 in KeyedServiceFactory::ContextDestroyed(void*) components/keyed_service/core/keyed_service_factory.cc:107:3
    #3 0x55b628e43363 in DependencyManager::PerformInterlockedTwoPhaseShutdown(DependencyManager*, void*, DependencyManager*, void*) components/keyed_service/core/dependency_manager.cc:154:14
    #4 0x55b624268803 in ProfileImpl::~ProfileImpl() chrome/browser/profiles/profile_impl.cc:909:3
    #5 0x55b624268f7d in ProfileImpl::~ProfileImpl() chrome/browser/profiles/profile_impl.cc:856:29
    #6 0x55b62427111b in ProfileDestroyer::DestroyOriginalProfileNow(Profile*) chrome/browser/profiles/profile_destroyer.cc:133:3
    #7 0x55b62427061f in ProfileDestroyer::DestroyProfileWhenAppropriate(Profile*) chrome/browser/profiles/profile_destroyer.cc:61:5
    #8 0x55b6242c0e9c in ProfileManager::ProfileInfo::~ProfileInfo() chrome/browser/profiles/profile_manager.cc:1645:3
    #9 0x55b6242c948e in std::__1::__tree<std::__1::__value_type<base::FilePath, std::__1::unique_ptr<ProfileManager::ProfileInfo, std::__1::default_delete<ProfileManager::ProfileInfo> > >, std::__1::__map_value_compare<base::FilePath, std::__1::__value_type<base::FilePath, std::__1::unique_ptr<ProfileManager::ProfileInfo, std::__1::default_delete<ProfileManager::ProfileInfo> > >, std::__1::less<base::FilePath>, true>, std::__1::allocator<std::__1::__value_type<base::FilePath, std::__1::unique_ptr<ProfileManager::ProfileInfo, std::__1::default_delete<ProfileManager::ProfileInfo> > > > >::erase(std::__1::__tree_const_iterator<std::__1::__value_type<base::FilePath, std::__1::unique_ptr<ProfileManager::ProfileInfo, std::__1::default_delete<ProfileManager::ProfileInfo> > >, std::__1::__tree_node<std::__1::__value_type<base::FilePath, std::__1::unique_ptr<ProfileManager::ProfileInfo, std::__1::default_delete<ProfileManager::ProfileInfo> > >, void*>*, long>) buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
    #10 0x55b6242bd93d in ProfileManager::RemoveProfile(base::FilePath const&) buildtools/third_party/libc++/trunk/include/__tree:2445:5
    #11 0x55b6242bd5d2 in ProfileManager::DeleteProfileIfNoKeepAlive(ProfileManager::ProfileInfo const*) chrome/browser/profiles/profile_manager.cc:1472:3
    #12 0x55b6242bcf27 in ProfileManager::RemoveKeepAlive(Profile const*, ProfileKeepAliveOrigin) chrome/browser/profiles/profile_manager.cc:1434:3
    #13 0x55b624d9edc3 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&) base/callback.h:142:12
    #14 0x55b624dd9773 in

base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*) base/task/common/task_annotator.h:74:5
    #15 0x55b624dd8f87 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:261:30
    #16 0x55b624dda341 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
    #17 0x55b624c961e9 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) base/message_loop/message_pump_glib.cc:375:46
    #18 0x7f1f132d6196 in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x4a196)
previously allocated by thread T0 (chrome) here:
    #0 0x55b616b4ba3d in operator new(unsigned long) third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:95:3
    #1 0x55b62476928f in StorageNotificationServiceFactory::BuildServiceInstanceFor(content::BrowserContext*) const buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:725:28
    #2 0x55b628e4905b in KeyedServiceFactory::GetServiceForContext(void*, bool) components/keyed_service/core/keyed_service_factory.cc:80:15
    #3 0x55b6247691c5 in StorageNotificationServiceFactory::GetForBrowserContext(content::BrowserContext*) chrome/browser/storage/storage_notification_service_factory.cc:21:22
    #4 0x55b61cb1b1f6 in content::StoragePartitionImpl::Initialize(content::StoragePartitionImpl*) content/browser/storage_partition_impl.cc:1170:25
    #5 0x55b61cb4e798 in content::StoragePartitionImplMap::Get(content::StoragePartitionConfig const&, bool) content/browser/storage_partition_impl_map.cc:352:14
    #6 0x55b61b99db3a in content::BrowserContext::GetDefaultStoragePartition() content/browser/browser_context.cc:139:52
    #7 0x55b623fbd9a4 in OptimizationGuideKeyedService::Initialize() chrome/browser/optimization_guide/optimization_guide_keyed_service.cc:110:35
    #8 0x55b623fbd6e1 in OptimizationGuideKeyedServiceFactory::BuildServiceInstanceFor(content::BrowserContext*) const chrome/browser/optimization_guide/optimization_guide_keyed_service_factory.cc:59:14
    #9 0x55b628e4905b in KeyedServiceFactory::GetServiceForContext(void*, bool) components/keyed_service/core/keyed_service_factory.cc:80:15
    #10 0x55b628e422c7 in DependencyManager::CreateContextServices(void*, bool) components/keyed_service/core/dependency_manager.cc
    #11 0x55b62ce4c8e3 in BrowserContextDependencyManager::CreateBrowserContextServices(content::BrowserContext*) components/keyed_service/content/browser_context_dependency_manager.cc:46:22
    #12 0x55b62426afe1 in ProfileImpl::OnLocaleReady(Profile::CreateMode) chrome/browser/profiles/profile_impl.cc:1104:51
    #13 0x55b624263cd6 in ProfileImpl::OnPrefsLoaded(Profile::CreateMode, bool) chrome/browser/profiles/profile_impl.cc:1145:3
    #14 0x55b6242628cf in ProfileImpl::ProfileImpl(base::FilePath const&, Profile::Delegate*, Profile::CreateMode, base::Time, scoped_refptr<base::SequencedTaskRunner>) chrome/browser/profiles/profile_impl.cc:535:5
    #15 0x55b62425f119 in Profile::CreateProfile(base::FilePath const&, Profile::Delegate*, Profile::CreateMode) chrome/browser/profiles/profile_impl.cc:365:59
    #16 0x55b6242add02 in ProfileManager::CreateAndInitializeProfile(base::FilePath const&) chrome/browser/profiles/profile_manager.cc:1788:38
    #17 0x55b6242aac67 in ProfileManager::GetProfile(base::FilePath const&) chrome/browser/profiles/profile_manager.cc:741:10
    #18 0x55b62f25aa36 in GetStartupProfile(base::FilePath const&, base::CommandLine const&) chrome/browser/ui/startup/startup_browser_creator.cc:1356:39
    #19 0x55b623d5633a in (anonymous namespace)::CreatePrimaryProfile(content::MainFunctionParams const&, base::FilePath const&, base::CommandLine const&) chrome/browser/chrome_browser_main.cc:418:18
    #20 0x55b623d534ba in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome/browser/chrome_browser_main.cc:1435:37
    #21 0x55b623d529d4 in ChromeBrowserMainParts::PreMainMessageLoopRun()

chrome/browser/chrome_browser_main.cc:1084:18
    #22 0x55b61ba2b34f in content::BrowserMainLoop::PreMainMessageLoopRun()
content/browser/browser_main_loop.cc:951:28
    #23 0x55b61cb15928 in content::StartupTaskRunner::RunAllTasksNow() base/callback.h:142:12
    #24 0x55b61ba2a98d in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:859:25
    #25 0x55b61ba3110f in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams)
content/browser/browser_main_runner_impl.cc:132:15
    #26 0x55b61ba2732e in content::BrowserMain(content::MainFunctionParams) content/browser/browser_main.cc:26:32
    #27 0x55b623b6c8b0 in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*) content/app/content_main_runner_impl.cc:646:10
    #28 0x55b623b6f97a in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
content/app/content_main_runner_impl.cc:1159:10
    #29 0x55b623b6ea52 in content::ContentMainRunnerImpl::Run() content/app/content_main_runner_impl.cc:1026:12
SUMMARY: AddressSanitizer: heap-use-after-free base/bind_internal.h:535:12 in
base::internal::Invoker<base::internal::BindState<void (content::StorageNotificationService::*)(url::Origin),
base::internal::UnretainedWrapper<content::StorageNotificationService>, url::Origin>, void
()>::RunOnce(base::internal::BindStateBase*)
Shadow bytes around the buggy address:
  0x0c08800c8b00: fa fa fa fa fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c08800c8b10: fa fa fa fa fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c08800c8b20: fa fa fa fa fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c08800c8b30: fa fa fa fa fd fd fd fd fa fa fa fa fd fd fd fd
  0x0c08800c8b40: fa fa fa fa 00 00 00 00 fa fa fa fa 00 00 00 00
=>0x0c08800c8b50: fa fa fa fa[fd]fd fd fa fa fa fa fa 00 00 00 00
  0x0c08800c8b60: fa fa fa fa 00 00 00 fa fa fa fa fa fd fd fd fa
  0x0c08800c8b70: fa fa fa fa 00 00 00 00 fa fa fa fa 00 00 00 00
  0x0c08800c8b80: fa fa fa fa fd fd fd fa fa fa fa fa fd fd fd fa
  0x0c08800c8b90: fa fa fa fa fd fd fd fd fa fa fa fa fd fd fd fa
  0x0c08800c8ba0: fa fa fa fa fd fd fd fa fa fa fa fa 00 00 00 fa
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone: fa
  Freed heap region: fd
  Stack left redzone: f1
  Stack mid redzone: f2
  Stack right redzone: f3
  Stack after return: f5
  Stack use after scope: f8
  Global redzone: f9
  Global init order: f6
  Poisoned by user: f7
  Container overflow: fc
  Array cookie: ac
  Intra object redzone: bb
  ASan internal: fe
  Left alloca redzone: ca
  Right alloca redzone: cb
==329557==ABORTING

Did this work before? N/A

Chrome version: 100.0.4676.0 Channel: n/a
OS Version: 10.0

clusterfuzz-testcase-6255222588243968.zip
80.9 KB Download

[Deleted] **asan.txt**

Comment 1 by sheriffbot on Tue, Nov 30, 2021, 3:48 AM EST Project Member

Labels: external_security_report

Comment 2 by m.coo...@gmail.com on Tue, Nov 30, 2021, 4:34 AM EST

upload asan log

asan.txt
31.1 KB View Download

Comment 3 by ClusterFuzz on Tue, Nov 30, 2021, 1:46 PM EST Project Member

Labels: Stability-Memory-AddressSanitizer

Detailed Report: https://clusterfuzz.com/testcase?key=6255222588243968

Fuzzer: b0ring_webidl_fuzzer
Job Type: linux_lsan_chrome_mp
Platform Id: linux

Crash Type: Heap-use-after-free READ 8
Crash Address: 0x604000685aa0
Crash State:
  base::internal::Invoker<base::internal::BindState<void
  base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImp
  base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork

Sanitizer: address (ASAN)

Recommended Security Severity: Critical

Crash Revision: https://clusterfuzz.com/revisions?job=linux_lsan_chrome_mp&revision=945738

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=6255222588243968

To reproduce this, please build the target in this report and run it against the reproducer testcase. Please use the GN arguments provided at bottom of this report when building the binary.

If you have trouble reproducing, please also export the environment variables listed under "[Environment]" in the crash stacktrace.

If you have any feedback on reproducing test cases, let us know at https://forms.gle/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 4 by ClusterFuzz on Tue, Nov 30, 2021, 1:54 PM EST Project Member

Labels: Test-Predator-Auto-Components
Components: Internals>Core Internals>SequenceManager

Automatically applying components based on crash stacktrace and information from OWNERS files.

If this is incorrect, please apply the Test-Predator-Wrong-Components label.

Comment 5 by ClusterFuzz on Tue, Nov 30, 2021, 1:54 PM EST Project Member

Labels: Unreproducible

ClusterFuzz testcase 6255222588243968 appears to be flaky, updating reproducibility label.

Comment 6 by m.coo...@gmail.com on Tue, Nov 30, 2021, 10:41 PM EST

Patching some code creates an case that is easier to reproduce.
#Tips
If MaybeShowStoragePressureNotification appears before Disassociate, then continue to increase the number of fuzz-00601.html pages to create

#Repro
E:\v8\chro2\src\out\asan>chrome --js-flags='--expose_gc --allow-natives-syntax' --no-sandbox --enable-blink-test-features --disable-extensions --user-data-dir=test D:\tmp\2021\11\clusterfuzz-testcase-6255222588243968\fuzz-00601.html D:\tmp\2021\11\clusterfuzz-testcase-6255222588243968\fuzz-00601.html D:\tmp\2021\11\clusterfuzz-testcase-6255222588243968\fuzz-00601.html

rep.diff
3.9 KB View Download

rep_asan.txt
51.5 KB View Download

Comment 7 by jdeblasio@chromium.org on Wed, Dec 1, 2021, 3:06 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: jarrydg@chromium.org
Labels: FoundIn-96 Security_Severity-Critical OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Lacros Pri-0

Thanks for the report and the analysis.

jarrydg@: this is code that you've worked on recently. Can you please take a look as soon as possible? If you're not the right person, please forward on appropriately.

Albeit flaky, this is a web-accessible use-after-free in the browser process, which is critical severity.

Comment 8 by jdeblasio@chromium.org on Wed, Dec 1, 2021, 3:07 PM EST Project Member

Components: -Internals>Core -Internals>SequenceManager Blink>Storage

Comment 9 by jdeblasio@chromium.org on Wed, Dec 1, 2021, 3:08 PM EST Project Member

Cc: mek@chromium.org

(+mek for visibility)

Comment 10 by sheriffbot on Wed, Dec 1, 2021, 3:12 PM EST Project Member

Labels: Security_Impact-Extended

Comment 11 by sheriffbot on Thu, Dec 2, 2021, 12:47 PM EST Project Member

Labels: Target-96 M-96

Setting milestone and target because of high severity.

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

Comment 12 by sheriffbot on Tue, Dec 14, 2021, 11:42 AM EST Project Member

Pri-0 bugs are critical regressions or serious emergencies, and this bug has not been updated in three days. Could you please provide an update, or adjust the priority to a more appropriate level if applicable?

If a fix is in active development, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 13 by jarrydg@chromium.org on Thu, Dec 16, 2021, 1:25 PM EST Project Member

Cc: dmu...@chromium.org

Comment 14 by dcheng@chromium.org on Thu, Dec 16, 2021, 2:16 PM EST Project Member

I think the problem here is the outer Unretained might be safe--after all, QuotaManager won't run the repeating callback if it's destroyed.

The problem is the inner callback also uses Unretained, but it's posting a task.

Comment 15 by dmu...@chromium.org on Thu, Dec 16, 2021, 2:26 PM EST Project Member

Yes - the posted task here is what is outliving the profile as far as I can tell.

Repeating callback makes this a little weird - but basically there needs to be a repeating callback that holds a weakptr that is only run on the UI thread, and another repeating callback that can be used from any thread which calls the UI thread one. The weird part is that the UI thread one also has to be destroyed on the UI thread (I believe? due to owning that weak ptr?)

Comment 16 by danakj@chromium.org on Thu, Dec 16, 2021, 3:28 PM EST Project Member

WeakPtr can be destroyed anywhere, it can only be queried/dereffed on the thread where the factory lives.

Comment 17 by dmu...@chromium.org on Thu, Dec 16, 2021, 4:24 PM EST Project Member

Wonderful! Then it shouldn't be that hard here.

Comment 18 by jarrydg@chromium.org on Sun, Dec 19, 2021, 7:06 PM EST Project Member

Cc: pwnall@chromium.org

Comment 19 by jarrydg@chromium.org on Mon, Dec 20, 2021, 2:27 PM EST Project Member

Cc: nasko@chromium.org jsb...@chromium.org

Comment 20 by Git Watcher on Tue, Dec 21, 2021, 7:08 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e304c0373f9cc4a65d39d7094e4897627e83390e

commit e304c0373f9cc4a65d39d7094e4897627e83390e
Author: Jarryd <jarrydg@chromium.org>
Date: Wed Dec 22 00:07:37 2021

Quota: Use Threadsafe Pressure Callback.

Fixes UAF by removing use of raw ptr to StorageNotificationService.
Instead, the service's interface exposes a method to create a
thread-safe callback to pass to the quota manager instead.

This change also changes the parameter type for the call chain from
url::Origin to blink::StorageKey to match the type Quota is keyed on.

~~Bug:1275020~~

Change-Id: Icc696d22fa41324e7a6c056599db635bb5de6291
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347939
Reviewed-by: Joshua Bell <jsbell@chromium.org>
Reviewed-by: Nasko Oskov <nasko@chromium.org>
Commit-Queue: Jarryd Goodman <jarrydg@chromium.org>
Cr-Commit-Position: refs/heads/main@{#953375}

[modify]
https://crrev.com/e304c0373f9cc4a65d39d7094e4897627e83390e/chrome/browser/storage/storage_notification_service_impl.cc
[modify]
https://crrev.com/e304c0373f9cc4a65d39d7094e4897627e83390e/content/public/browser/storage_notification_service.h
[modify] https://crrev.com/e304c0373f9cc4a65d39d7094e4897627e83390e/content/browser/storage_partition_impl.cc
[modify]
https://crrev.com/e304c0373f9cc4a65d39d7094e4897627e83390e/chrome/browser/storage/storage_notification_service_impl.h

Comment 21 by wfh@chromium.org on Tue, Dec 21, 2021, 11:34 PM EST Project Member

[sheriff] Please mark bug as fixed if #20 fixed it, so merge(s) can be picked up. Thank you.

Comment 22 by jarrydg@chromium.org on Thu, Dec 23, 2021, 10:43 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 23 by sheriffbot on Thu, Dec 23, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 24 by sheriffbot on Thu, Dec 23, 2021, 1:40 PM EST Project Member

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

Comment 25 by sheriffbot on Thu, Dec 23, 2021, 2:01 PM EST Project Member

Labels: Merge-Request-96 Merge-Request-97 Merge-Request-98

Requesting merge to stable M96 because latest trunk commit (953375) appears to be after stable branch point (929512).

Requesting merge to beta M97 because latest trunk commit (953375) appears to be after beta branch point (938553).

Requesting merge to dev M98 because latest trunk commit (953375) appears to be after dev branch point (950365).

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

Comment 26 by sheriffbot on Thu, Dec 23, 2021, 2:01 PM EST Project Member

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

Merge review required: M97 has already been cut for stable release.

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

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

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

Comment 27 by sheriffbot on Thu, Dec 23, 2021, 2:01 PM EST Project Member

Labels: -Merge-Request-96 Merge-Review-96

Merge review required: M96 is already shipping to stable.

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

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 28 by sheriffbot on Thu, Dec 23, 2021, 2:07 PM EST Project Member

Labels: -Merge-Request-98 Hotlist-Merge-Approved Merge-Approved-98

Merge approved: your change passed merge requirements and is auto-approved for M98. Please go ahead and merge the CL to branch 4758 (refs/branch-heads/4758) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 29 by sheriffbot on Mon, Dec 27, 2021, 12:21 PM EST Project Member

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 30 by pbommana@google.com on Mon, Dec 27, 2021, 12:56 PM EST Project Member

Cc: adetaylor@chromium.org amyressler@chromium.org

+Adetaylor and Amyressler@ Security TPM's for merge review as this is marked as Security_Severity-Critical and P0

Comment 31 by amyressler@chromium.org on Mon, Dec 27, 2021, 3:29 PM EST Project Member

Cc: -adetaylor@chromium.org
Labels: -Merge-Review-96 -Merge-Review-97 Merge-Approved-97 Merge-Approved-96

this was already approved for merge to M98, please merge to branch 4758 as soon as possible
tentatively approving for merge to M97; please confirm there are no stability issues or other concerns with this fix since it's been on canary for approximately five days now. Once confirmed please merge to branch 4692 as soon as possible.
Since this is a critical severity fix, please merge to branch 4664 so that it can be included in M96 as it will be on extended support. Thank you.

Comment 32 by pbommana@google.com on Tue, Dec 28, 2021, 3:33 PM EST Project Member

Cc: benmason@chromium.org gov...@chromium.org pbomm...@chromium.org
Labels: OS-Android

Tentatively tagging the bug with OS-Android sine this is a issue in Blink, jarrydg@ can you please confirm and remove Android if not applicable.

Comment 33 by gov...@chromium.org on Tue, Dec 28, 2021, 4:15 PM EST Project Member

Cc: marinakz@chromium.org

Comment 34 by gov...@chromium.org on Tue, Dec 28, 2021, 4:24 PM EST Project Member

Cc: pbommana@google.com

Prepared merge to M96, M97 and M98 and put it in CQ dry run. Please DO NOT merge yet until we get canary stability confirmation from +pbommana@.

* M96: https://chromium-review.googlesource.com/c/chromium/src/+/3360203

* M97:https://chromium-review.googlesource.com/c/chromium/src/+/3360202
* M98: https://chromium-review.googlesource.com/c/chromium/src/+/3360201

Comment 35 by Git Watcher on Tue, Dec 28, 2021, 5:47 PM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e531a38cf5fd45997b5f60b1d4a3c58126996b73

commit e531a38cf5fd45997b5f60b1d4a3c58126996b73
Author: Jarryd <jarrydg@chromium.org>
Date: Tue Dec 28 22:46:20 2021

Quota: Use Threadsafe Pressure Callback.

Fixes UAF by removing use of raw ptr to StorageNotificationService.
Instead, the service's interface exposes a method to create a
thread-safe callback to pass to the quota manager instead.

This change also changes the parameter type for the call chain from
url::Origin to blink::StorageKey to match the type Quota is keyed on.

~~Bug:1275020~~

(cherry picked from commit e304c0373f9cc4a65d39d7094e4897627e83390e)

Change-Id: Icc696d22fa41324e7a6c056599db635bb5de6291
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347939
Reviewed-by: Joshua Bell <jsbell@chromium.org>
Reviewed-by: Nasko Oskov <nasko@chromium.org>
Commit-Queue: Jarryd Goodman <jarrydg@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#953375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3360201
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Owners-Override: Krishna Govind <govind@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/4758@{#257}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify]
https://crrev.com/e531a38cf5fd45997b5f60b1d4a3c58126996b73/chrome/browser/storage/storage_notification_service_impl.cc
[modify]
https://crrev.com/e531a38cf5fd45997b5f60b1d4a3c58126996b73/content/public/browser/storage_notification_service.h
[modify] https://crrev.com/e531a38cf5fd45997b5f60b1d4a3c58126996b73/content/browser/storage_partition_impl.cc
[modify]
https://crrev.com/e531a38cf5fd45997b5f60b1d4a3c58126996b73/chrome/browser/storage/storage_notification_service_impl.h

Comment 36 by Git Watcher on Tue, Dec 28, 2021, 6:21 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6122b68dfd0437e5576889466f4c0c34158a14ef

commit 6122b68dfd0437e5576889466f4c0c34158a14ef
Author: Jarryd <jarrydg@chromium.org>
Date: Tue Dec 28 23:20:39 2021

Quota: Use Threadsafe Pressure Callback.

Fixes UAF by removing use of raw ptr to StorageNotificationService.
Instead, the service's interface exposes a method to create a
thread-safe callback to pass to the quota manager instead.

This change also changes the parameter type for the call chain from
url::Origin to blink::StorageKey to match the type Quota is keyed on.

~~Bug:1275020~~

(cherry picked from commit e304c0373f9cc4a65d39d7094e4897627e83390e)

Change-Id: Icc696d22fa41324e7a6c056599db635bb5de6291
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347939
Reviewed-by: Joshua Bell <jsbell@chromium.org>
Reviewed-by: Nasko Oskov <nasko@chromium.org>
Commit-Queue: Jarryd Goodman <jarrydg@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#953375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3360202
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Owners-Override: Krishna Govind <govind@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/4692@{#1243}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify]
https://crrev.com/6122b68dfd0437e5576889466f4c0c34158a14ef/chrome/browser/storage/storage_notification_service_impl.cc
[modify]
https://crrev.com/6122b68dfd0437e5576889466f4c0c34158a14ef/content/public/browser/storage_notification_service.h
[modify] https://crrev.com/6122b68dfd0437e5576889466f4c0c34158a14ef/content/browser/storage_partition_impl.cc
[modify]
https://crrev.com/6122b68dfd0437e5576889466f4c0c34158a14ef/chrome/browser/storage/storage_notification_service_impl.h

Comment 37 by Git Watcher on Wed, Dec 29, 2021, 2:50 PM EST Project Member

Labels: -merge-approved-96 merge-merged-4664 merge-merged-96

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c5571653d9323402e7ab316f97e675b8e7f2c6e1

commit c5571653d9323402e7ab316f97e675b8e7f2c6e1
Author: Jarryd <jarrydg@chromium.org>
Date: Wed Dec 29 19:49:22 2021

Quota: Use Threadsafe Pressure Callback.

Fixes UAF by removing use of raw ptr to StorageNotificationService.
Instead, the service's interface exposes a method to create a
thread-safe callback to pass to the quota manager instead.

This change also changes the parameter type for the call chain from
url::Origin to blink::StorageKey to match the type Quota is keyed on.

~~Bug:1275020~~

(cherry picked from commit e304c0373f9cc4a65d39d7094e4897627e83390e)

Change-Id: Icc696d22fa41324e7a6c056599db635bb5de6291
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3347939
Reviewed-by: Joshua Bell <jsbell@chromium.org>
Reviewed-by: Nasko Oskov <nasko@chromium.org>
Commit-Queue: Jarryd Goodman <jarrydg@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#953375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3360203
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Owners-Override: Krishna Govind <govind@chromium.org>
Commit-Queue: Krishna Govind <govind@chromium.org>
Cr-Commit-Position: refs/branch-heads/4664@{#1352}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/c5571653d9323402e7ab316f97e675b8e7f2c6e1/chrome/browser/storage/storage_notification_service_impl.cc
[modify]
https://crrev.com/c5571653d9323402e7ab316f97e675b8e7f2c6e1/content/public/browser/storage_notification_service.h
[modify] https://crrev.com/c5571653d9323402e7ab316f97e675b8e7f2c6e1/content/browser/storage_partition_impl.cc
[modify]
https://crrev.com/c5571653d9323402e7ab316f97e675b8e7f2c6e1/chrome/browser/storage/storage_notification_service_impl.h

Comment 38 by amyressler@chromium.org on Tue, Jan 4, 2022, 11:51 AM EST Project Member

Labels: Release-0-M97

Comment 39 by amyressler@google.com on Tue, Jan 4, 2022, 1:33 PM EST Project Member

Labels: CVE-2022-0096 CVE_description-missing

Comment 40 by amyressler@google.com on Wed, Jan 5, 2022, 8:01 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-20000

*** 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 41 by amyressler@chromium.org on Wed, Jan 5, 2022, 8:03 PM EST Project Member

Congratulations! The VRP Panel has decided to award you $20,000 for this report. Thank you for your efforts in reporting this critical issue and great work!

Comment 42 by amyressler@google.com on Thu, Jan 6, 2022, 3:47 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 43 by sheriffbot on Thu, Mar 31, 2022, 1:29 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

Comment 44 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted