




☆ Starred by 4 users

Owner:  asully@chromium.org
OOO until Dec 19th

CC:  asully@chromium.org
mek@chromium.org
 pwnall@chromium.org

Status: Fixed (Closed)

Components: [Blink>Storage>FileSystem](#)

Modified: Dec 19, 2021

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: [Linux](#), [Android](#), [Windows](#), [Chrome](#), [Mac](#), [Fuchsia](#), [Lacros](#)

Pri: 1

Type: [Bug-Security](#)

[Hotlist-Merge-Review](#)
[Security_Severity-Medium](#)
[Hotlist-Merge-Approved](#)
[allpublic](#)
[reward-inprocess](#)
[reward-15000](#)
[CVE_description-submitted](#)
[external_security_report](#)
[Target-94](#)
[M-94](#)
[merge-merged-4430](#)
[FoundIn-93](#)
[LTS-Merged-90](#)
[LTS-Security-90](#)
[LTS-Size-Small](#)
[LTS-Complexity-Trivial](#)
[Security_Impact-Extended](#)
[merge-merged-4606](#)
[merge-merged-94](#)
[Release-0-M94](#)
[merge-merged-4638](#)
[merge-merged-95](#)
[CVE-2021-37970](#)

Issue 1248030: Security: Use After Free in FileSystemAccessManagerImpl

Reported by soulc...@gmail.com on Thu, Sep 9, 2021, 8:21 AM EDT

 Code

This template is ONLY for reporting security bugs. If you are reporting a Download Protection Bypass bug, please use the "Security - Download Protection" template. For all other reports, please use a different template.

Please READ THIS FAQ before filing a bug: <https://chromium.googlesource.com/chromium/src/+HEAD/docs/security/faq.md>

Please see the following link for instructions on filing security bugs: <https://www.chromium.org/Home/chromium-security/reporting-security-bugs>

Reports may be eligible for reward payments under the Chrome VRP: <http://g.co/ChromeBugRewards>

NOTE: Security bugs are normally made public once a fix has been widely deployed.

VULNERABILITY DETAILS

In class FileSystemAccessManagerImpl, there is a raw pointer:

```
====  
FileSystemAccessPermissionContext* permission_context_  
=====
```

'permission_context_' is owned by StoragePartitionImpl, on the other hand, FileSystemAccessManagerImpl is owned by StoragePartitionImpl too from annotation(in face it is NOT):

```
====  
// This is the browser side implementation of the  
// FileSystemAccessManager mojom interface. This is the main entry point for  
// the File System Access API in the browser process. Instances of this class are  
// owned by StoragePartitionImpl.  
=====
```

So in normal situation, the raw pointer 'permission_context_' in FileSystemAccessManagerImpl is safe. But FileSystemAccessManagerImpl is a RefCountedThreadSafe object so in special situation, we can add ref to it and outlives of StoragePartitionImpl, and the raw pointer 'permission_context_' becomes dangling pointer.

In function 'FileSystemAccessManagerImpl::DidVerifySensitiveDirectoryAccess', there are some 'base::BindOnce' call with argument 'this', this will add ref of FileSystemAccessManagerImpl.

```
=====
```

```
operation_runner().PostTaskWithThisObject(
    FROM_HERE,
    base::BindOnce(
        &CreateAndTruncateFile, fs_url,
        base::BindOnce(
            &FileSystemAccessManagerImpl::DidCreateAndTruncateSaveFile,
            this, binding_context, entries.front(), fs_url,
            std::move(callback)),
        base::SequencedTaskRunnerHandle::Get());
}
```

So consider below situation, uaf will happen:

1. call above BindOnce function, ref count is 2, and then post task DidCreateAndTruncateSaveFile.
2. call ~StoragePartitionImpl, frees FileSystemAccessPermissionContext, and 'permission_context_' becomes dangling pointer, FileSystemAccessManagerImpl's ref count is 1 so it still lives.
3. call 'DidCreateAndTruncateSaveFile' => 'GetSharedHandleStateForPath' => 'permission_context_->GetReadPermissionGrant' and uaf happens.

how to reproduce:

```
$python /copy_mojo_js_bindings.py /path/to/chrome/.../out/Debug/gen
$out/Debug/chrome --enable-blink-features=MojoJS 127.0.0.1:8000/1.html
$click trigger, wait about 4-8 seconds(it need to race here and depend on hardware, so may be it is not stable to reproduce, if you can't, change the time here), and click
confirm save file.
```

The fix:

I think the FileSystemAccessManagerImpl need to create a 'Shutdown' function like FileSystemContext and ~StoragePartitionImpl will call it. In 'Shutdown' function, it will clear the raw pointer 'permission_context_'. There are many places like 'if (permission_context_)' in FileSystemAccessManagerImpl's methods, so I think you may be forget to create a 'Shutndown' function for FileSystemAccessManagerImpl.

*Please note that this bug may be can trigger with normal render process(not compromised) as the mojo interfaces can be called from web API. I use MojoJS just a convenience and for race more stable. It is not necessary.

As it need to race to trigger the bug, so may be it is not stable to reproduce, please try more times. But the bug is clear in code.

VERSION

Chrome Version: [x.x.x.x] + [stable, beta, or dev]

Operating System: [Please indicate OS, version, and service pack level]

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION

Type of crash:browser

Crash State:

==780772==ERROR: AddressSanitizer: heap-use-after-free on address 0x12195242be40 at pc 0x7ff82e6009cf bp 0x00076f1fe7c0 sp 0x00076f1fe808

READ of size 8 at 0x12195242be40 thread T0

```
#0 0x7ff82e6009ce in content::FileSystemAccessManagerImpl::GetSharedHandleStateForPath(class base::FilePath const &, class url::Origin const &, enum
content::FileSystemAccessPermissionContext::HandleType, enum content::FileSystemAccessPermissionContext::UserAction)
src/content/browser/file_system_access/file_system_access_manager_impl.cc:1377:39
```

```
#1 0x7ff82e60a5e4 in content::FileSystemAccessManagerImpl::DidCreateAndTruncateSaveFile(struct content::FileSystemAccessEntryFactory::BindingContext const &,
struct content::FileSystemChooser::ResultEntry const &, class storage::FileSystemURL const &, class base::OnceCallback<(class mojo::InlinedStructPtr<class
blink::mojom::FileSystemAccessError>, class std::__1::vector<class mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>, class std::__1::allocator<class
mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>>>>>, bool) src/content/browser/file_system_access/file_system_access_manager_impl.cc:1253:43
#2 0x7ff82e61de3e in base::internal::FunctorTraits<void (content::FileSystemAccessManagerImpl::*)(const content::FileSystemAccessEntryFactory::BindingContext &,
const content::FileSystemChooser::ResultEntry &, const storage::FileSystemURL &, base::OnceCallback<void
(mojom::InlinedStructPtr<blink::mojom::FileSystemAccessError>,
std::__1::vector<mojo::StructPtr<blink::mojom::FileSystemAccessEntry>, std::__1::allocator<mojo::StructPtr<blink::mojom::FileSystemAccessEntry> > >>, bool), void>::Invoke
src/base/bind_internal.h:509
```

```
#3 0x7ff82e61de3e in base::internal::InvokeHelper<0, void>::MakeItSo src/base/bind_internal.h:648
```

```
#4 0x7ff82e61de3e in base::internal::Invoker<base::internal::BindState<void (content::FileSystemAccessManagerImpl::*)(const
content::FileSystemAccessEntryFactory::BindingContext &, const content::FileSystemChooser::ResultEntry &, const storage::FileSystemURL &, base::OnceCallback<void
(mojom::InlinedStructPtr<blink::mojom::FileSystemAccessError>,
std::__1::vector<mojo::StructPtr<blink::mojom::FileSystemAccessEntry>, std::__1::allocator<mojo::StructPtr<blink::mojom::FileSystemAccessEntry> > >>,
bool), scoped_refptr<content::FileSystemAccessManagerImpl>>, class std::__1::allocator<class mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>>>>, bool), class scoped_refptr<class
content::FileSystemAccessManagerImpl>, struct content::FileSystemAccessEntryFactory::BindingContext, struct content::FileSystemChooser::ResultEntry, class
storage::FileSystemURL, class base::OnceCallback<void ____cdecl(class mojom::InlinedStructPtr<class blink::mojom::FileSystemAccessError>, class std::__1::vector<class
mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>, class std::__1::allocator<class mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>>>>>>,
(bool)>::RunImpl src/base/bind_internal.h:721
```

```
#5 0x7ff82e61de3e in base::internal::Invoker<struct base::internal::BindState<void (____cdecl content::FileSystemAccessManagerImpl::*)(struct
content::FileSystemAccessEntryFactory::BindingContext const &, struct content::FileSystemChooser::ResultEntry const &, class storage::FileSystemURL const &, class
base::OnceCallback<(class mojom::InlinedStructPtr<class blink::mojom::FileSystemAccessError>, class std::__1::vector<class mojo::StructPtr<class
blink::mojom::FileSystemAccessEntry>, class std::__1::allocator<class mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>>>>>, bool), class scoped_refptr<class
content::FileSystemAccessManagerImpl>, struct content::FileSystemAccessEntryFactory::BindingContext, struct content::FileSystemChooser::ResultEntry, class
storage::FileSystemURL, class base::OnceCallback<void ____cdecl(class mojom::InlinedStructPtr<class blink::mojom::FileSystemAccessError>, class std::__1::vector<class
mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>, class std::__1::allocator<class mojo::StructPtr<class blink::mojom::FileSystemAccessEntry>>>>>>,
(bool)>::RunOnce(class base::internal::BindStateBase *, bool) src/base/bind_internal.h:690:12
```

```
#6 0x7ff829bccdee in base::OnceCallback<(bool)>::Run(bool) && src/base/callback.h:98:12
```

```
#7 0x7ff82bfb543 in base::internal::FunctorTraits<class base::OnceCallback<(bool)>, void>::Invoke<class base::OnceCallback<(bool)>, bool>::class
base::OnceCallback<(bool)> &&, bool &&) src/base/bind_internal.h:608:49
```

```
#8 0x7ff83689b16c in base::OnceCallback<void (>::Run src/base/callback.h:99
```

```
#9 0x7ff83689b16c in base::TaskAnnotator::RunTask(char const *, struct base::PendingTask *) src/base/task/common/task_annotator.cc:178:33
```

```
#10 0x7ff839a9ea6a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(class base::sequence_manager::LazyNow *)
```

```
src/base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:360:23
```

```
#11 0x7ff839a9d44d in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork(void)
```

```
src/base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:260:36
```

```
#12 0x7ff836981779 in base::MessagePumpForUI::DoRunLoop(void) src/base/message_loop/message_pump_win.cc:220:67
```

```
#13 0x7ff83697eaae in base::MessagePumpWin::Run(class base::MessagePump::Delegate *) src/base/message_loop/message_pump_win.cc:78:3
```

```
#14 0x7ff839aadddd in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, class base::TimeDelta)
```

```
src/base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:467:12
```

```
#15 0x7ff83681d7d5 in base::RunLoop::Run(class base::Location const &) src/base/run_loop.cc:134:14
```

```
#16 0x7ff82e0f6455 in content::BrowserMainLoop::RunMainMessageLoop(void) src/content/browser/browser_main_loop.cc:988:18
```

```
#17 0x7ff82e0fc8b1 in content::BrowserMainRunnerImpl::Run(void) src/content/browser/browser_main_runner_impl.cc:152:15
```

```
#18 0x7ff82e0eec68 in content::BrowserMain(struct content::MainFunctionParams const &) src/content/browser/browser_main.cc:49:28
```

```
#19 0x7ff83141708d in content::RunBrowserProcessMain(struct content::MainFunctionParams const &, class content::ContentMainDelegate *)
```

```
src/content/app/content_main_runner_impl.cc:608:10
```

```
#20 0x7ff83141a190 in content::ContentMainRunnerImpl::RunBrowser(struct content::MainFunctionParams &, bool) src/content/app/content_main_runner_impl.cc:1104:10
```

```
#21 0x7ff8314191cc in content::ContentMainRunnerImpl::Run(bool) src/content/app/content_main_runner_impl.cc:971:12
```

```
#22 0x7ff83141555f in content::RunContentProcess(struct content::ContentMainParams const &, class content::ContentMainRunner *)
```

```
src/content/app/content_main.cc:390:36
```

```
#23 0x7ff8314165cc in content::ContentMain(struct content::ContentMainParams const &) src/content/app/content_main.cc:418:10
```

```
#24 0x7ff8297a14a7 in ChromeMain src/chrome/app/chrome_main.cc:172:12
```

```
#25 0x7ff6221c7858 in MainDILoader::Launch(struct HINSTANCE __*, class base::TimeTicks) src/chrome/app/main_dll_loader_win.cc:169:12
```

```
#26 0x7ff6221c33a4 in main src/chrome/app/chrome_exe_main_win.cc:382:20
```

```
#27 0x7ff6226c88df in invoke_main d:\a01_work\2\src\tools\src\vcstartup\src\startup\exe_common.inl:78
```

```
#28 0x7ff6226c88df in __scrt_common_main_seh d:\a01_work\2\src\tools\src\vcstartup\src\startup\exe_common.inl:288
```

```
#29 0x7ff93ef87033 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
```

```
#30 0x7ff940b22650 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

0x12195242be40 is located 0 bytes inside of 448-byte region [0x12195242be40,0x12195242c000)
freed by thread T0 here:
#0 0x7ff62227943b in free C:\b\sw\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82
#1 0x7ff8429173ea in [thunk]: ChromeFileSystemAccessPermissionContext::vector deleting dtor<adjustor[8]{unsigned int} (src\out\ASAN_8_14\chrome.dll+0x1991773ea)
#2 0x7ff82d37b8bc in std::_1::default_delete<gpu::gles2::AbstractTexture>::operator() src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:54
#3 0x7ff82d37b8bc in std::_1::unique_ptr<gpu::gles2::AbstractTexture, std::_1::default_delete<gpu::gles2::AbstractTexture> >::~reset
src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:315
#4 0x7ff82d37b8bc in std::_1::unique_ptr<gpu::gles2::AbstractTexture, std::_1::default_delete<gpu::gles2::AbstractTexture> >::~unique_ptr
src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:269
#5 0x7ff82d37b8bc in std::_1::pair<const unsigned int, std::_1::unique_ptr<gpu::gles2::AbstractTexture, std::_1::default_delete<gpu::gles2::AbstractTexture> > >::~pair
src\buildtools\third_party\libc++\trunk\include\utility:394
#6 0x7ff82d37b8bc in std::_1::allocator_traits<std::_1::allocator<std::_1::tree_node<std::_1::value_type<unsigned
int, std::_1::unique_ptr<gpu::gles2::AbstractTexture, std::_1::default_delete<gpu::gles2::AbstractTexture> > >, void *> > >::destroy
src\buildtools\third_party\libc++\trunk\include\_memory\allocator_traits.h:318
#7 0x7ff82d37b8bc in std::_1::tree<struct std::_1::value_type<unsigned __int64, class std::_1::unique_ptr<class mojo::MessageReceiver, struct
std::_1::default_delete<class mojo::MessageReceiver>>>, class std::_1::map_value_compare<unsigned __int64, struct std::_1::value_type<unsigned __int64, class
std::_1::unique_ptr<class mojo::MessageReceiver, struct std::_1::default_delete<class mojo::MessageReceiver>>>, struct std::_1::less<unsigned __int64>, 1>, class
std::_1::allocator<struct std::_1::value_type<unsigned __int64, class std::_1::unique_ptr<class mojo::MessageReceiver, struct std::_1::default_delete<class
mojo::MessageReceiver>>>>>>::erase(class std::_1::tree_const_iterator<struct std::_1::value_type<unsigned __int64, class std::_1::unique_ptr<class
mojo::MessageReceiver, struct std::_1::default_delete<class mojo::MessageReceiver>>>, class std::_1::tree_node<struct std::_1::value_type<unsigned __int64,
class std::_1::unique_ptr<class mojo::MessageReceiver, struct std::_1::default_delete<class mojo::MessageReceiver>>>, void *> *, __int64)>)
src\buildtools\third_party\libc++\trunk\include\_tree:242:5
#8 0x7ff837c0289e in std::_1::map<void *, std::_1::unique_ptr<KeyedService, std::_1::default_delete<KeyedService> >, std::_1::less<void
*>, std::_1::allocator<std::_1::pair<void *const, std::_1::unique_ptr<KeyedService, std::_1::default_delete<KeyedService> > > > >::erase
src\buildtools\third_party\libc++\trunk\include\map:1314
#9 0x7ff837c0289e in KeyedServiceFactory::Disassociate(void *) src\components\keyed_service\core\keyed_service_factory.cc:97:14
#10 0x7ff837c02b2e in KeyedServiceFactory::ContextDestroyed(void *) src\components\keyed_service\core\keyed_service_factory.cc:107:3
#11 0x7ff83abe7bcb in DependencyManager::DestroyFactoriesInOrder src\components\keyed_service\core\dependency_manager.cc:151
#12 0x7ff83abe7bcb in DependencyManager::PerformInterlockedTwoPhaseShutdown(class DependencyManager *, void *, class DependencyManager *, void *)
src\components\keyed_service\core\dependency_manager.cc:127:3
#13 0x7ff839980a81 in ProfileImpl::~ProfileImpl(void) src\chrome\browser\profiles\profile_impl.cc:894:3
#14 0x7ff839985b09 in ProfileImpl::scalar deleting dtor<unsigned int> src\chrome\browser\profiles\profile_impl.cc:850:29
#15 0x7ff83999d49d in ProfileDestroyer::DestroyOriginalProfileNow(class Profile *const) src\chrome\browser\profiles\profile_destroyer.cc:133:3
#16 0x7ff83999abd4 in ProfileDestroyer::DestroyProfileWhenAppropriate(class Profile *const) src\chrome\browser\profiles\profile_destroyer.cc:61:5
#17 0x7ff836616992 in ProfileManager::ProfileInfo::~ProfileInfo(void) src\chrome\browser\profiles\profile_manager.cc:1600:3
#18 0x7ff8366276cd in std::_1::default_delete<ProfileManager::ProfileInfo>::operator() src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:54
#19 0x7ff8366276cd in std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class ProfileManager::ProfileInfo> >::~reset(class
ProfileManager::ProfileInfo *) src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:315:7
#20 0x7ff8366278ac in std::_1::unique_ptr<ProfileManager::ProfileInfo, std::_1::default_delete<ProfileManager::ProfileInfo> >::~unique_ptr
src\buildtools\third_party\libc++\trunk\include\_memory\unique_ptr.h:269
#21 0x7ff8366278ac in std::_1::pair<const base::FilePath, std::_1::unique_ptr<ProfileManager::ProfileInfo, std::_1::default_delete<ProfileManager::ProfileInfo> > >::~pair
src\buildtools\third_party\libc++\trunk\include\utility:394
#22 0x7ff8366278ac in
std::_1::allocator_traits<std::_1::allocator<std::_1::tree_node<std::_1::value_type<base::FilePath, std::_1::unique_ptr<ProfileManager::ProfileInfo, std::_1::default_
delete<ProfileManager::ProfileInfo> > >, void *> > >::destroy src\buildtools\third_party\libc++\trunk\include\_memory\allocator_traits.h:318
#23 0x7ff8366278ac in std::_1::tree<struct std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct
std::_1::default_delete<class ProfileManager::ProfileInfo>>>, class std::_1::map_value_compare<class base::FilePath, struct std::_1::value_type<class
base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class ProfileManager::ProfileInfo>>>, struct std::_1::less<class
base::FilePath>, 1>, class std::_1::allocator<struct std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct
std::_1::default_delete<class ProfileManager::ProfileInfo>>>>>>::erase(class std::_1::tree_const_iterator<struct std::_1::value_type<class base::FilePath, class
std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class ProfileManager::ProfileInfo>>>, class std::_1::tree_node<struct
std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class
ProfileManager::ProfileInfo>>>, void *> *, __int64>) src\buildtools\third_party\libc++\trunk\include\_tree:242:5
#24 0x7ff836627801 in std::_1::tree<struct std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct
std::_1::default_delete<class ProfileManager::ProfileInfo>>>, class std::_1::map_value_compare<class base::FilePath, struct std::_1::value_type<class
base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class ProfileManager::ProfileInfo>>>, struct std::_1::less<class
base::FilePath>, 1>, class std::_1::allocator<struct std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct
std::_1::default_delete<class ProfileManager::ProfileInfo>>>>>>::erase(class std::_1::tree_const_iterator<struct std::_1::value_type<class base::FilePath, class
std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class ProfileManager::ProfileInfo>>>, class std::_1::tree_node<struct
std::_1::value_type<class base::FilePath, class std::_1::unique_ptr<class ProfileManager::ProfileInfo, struct std::_1::default_delete<class
ProfileManager::ProfileInfo>>>, void *> *, __int64>) src\buildtools\third_party\libc++\trunk\include\_tree:244:5
#25 0x7ff83661ab63 in std::_1::map<base::FilePath, std::_1::unique_ptr<ProfileManager::ProfileInfo, std::_1::default_delete<ProfileManager::ProfileInfo>
>, std::_1::less<base::FilePath>, std::_1::allocator<std::_1::pair<const
base::FilePath, std::_1::unique_ptr<ProfileManager::ProfileInfo, std::_1::default_delete<ProfileManager::ProfileInfo> > > > >::erase
src\buildtools\third_party\libc++\trunk\include\map:1317
#26 0x7ff83661ab63 in ProfileManager::RemoveProfile(class base::FilePath const &) src\chrome\browser\profiles\profile_manager.cc:1705:18
#27 0x7ff83661a715 in ProfileManager::DeleteProfileIfNoKeepAlive(class ProfileManager::ProfileInfo const *) src\chrome\browser\profiles\profile_manager.cc:1428:3
#28 0x7ff836619f54 in ProfileManager::RemoveKeepAlive(class Profile const *, enum ProfileKeepAliveOrigin) src\chrome\browser\profiles\profile_manager.cc:1390:3
#29 0x7ff83ba86844 in ScopedProfileKeepAlive::RemoveKeepAliveOnUIThread(class Profile const *, enum ProfileKeepAliveOrigin)
src\chrome\browser\profiles\scoped_profile_keep_alive.cc:44:22
#30 0x7ff83689b16c in base::OnceCallback<void ()>::Run src\base\callback.h:99
#31 0x7ff83689b16c in base::TaskAnnotator::RunTask(char const *, struct base::PendingTask *) src\base\task\common\task_annotator.cc:178:33
#32 0x7ff839a9ea6a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(class base::sequence_manager::LazyNow *)
src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:360:23
#33 0x7ff839a9d4d4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork(void)
src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:260:36
#34 0x7ff836981779 in base::MessagePumpForUI::DoRunLoop(void) src\base\message_loop\message_pump_win.cc:220:67
#35 0x7ff83697eaae in base::MessagePumpWin::Run(class base::MessagePump::Delegate *) src\base\message_loop\message_pump_win.cc:78:3
#36 0x7ff839aa0dd4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, class base::TimeDelta)
src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:467:12
#37 0x7ff8368147d5 in base::RunLoop::Run(class base::Location const &) src\base\run_loop.cc:134:14
#38 0x7ff82e0f6455 in content::BrowserMainLoop::RunMainMessageLoop(void) src\content\browser\browser_main_loop.cc:988:18
#39 0x7ff82e0fc8b1 in content::BrowserMainRunnerImpl::Run(void) src\content\browser\browser_main_runner_impl.cc:152:15
#40 0x7ff82e0ec688 in content::BrowserMain(struct content::MainFunctionParams const &) src\content\browser\browser_main.cc:49:28
```

previously allocated by thread T0 here:

```
#0 0x7ff62227953b in malloc C:\b\sw\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
#1 0x7ff84c28acae in operator new(unsigned __int64) d:\a01\work\12\src\lcvtools\crt\vcstartup\src\heap\new_scalar.cpp:35
#2 0x7ff83d93a25e in FileSystemAccessPermissionContextFactory::BuildServiceInstanceFor(class content::BrowserContext *) const
src\chrome\browser\file_system_access\file_system_access_permission_context_factory.cc:56:10
#3 0x7ff83be127ad in BrowserContextKeyedServiceFactory::BuildServiceInstanceFor(void *) const
src\components\keyed_service\content\browser_context_keyed_service_factory.cc:95:7
#4 0x7ff837c01f3f in KeyedServiceFactory::GetServiceForContext(void *, bool) src\components\keyed_service\core\keyed_service_factory.cc:80:15
#5 0x7ff83d93a0da in FileSystemAccessPermissionContextFactory::GetForProfile(class content::BrowserContext *)
src\chrome\browser\file_system_access\file_system_access_permission_context_factory.cc:19:22
#6 0x7ff82f306830 in content::StoragePartitionImpl::Initialize(class content::StoragePartitionImpl *) src\content\browser\storage_partition_impl.cc:1244:29
#7 0x7ff82f348c22 in content::StoragePartitionImplMap::Get(class content::StoragePartitionConfig const &, bool)
src\content\browser\storage_partition_impl_map.cc:353:14
#8 0x7ff82e09eb88 in content::BrowserContext::GetStoragePartition(class content::StoragePartitionConfig const &, bool) src\content\browser\browser_context.cc:145:52
#9 0x7ff82e09f4ce in content::BrowserContext::GetDefaultStoragePartition(void) src\content\browser\browser_context.cc:187:10
#10 0x7ff841a34489 in OptimizationGuideKeyedService::Initialize(void) src\chrome\browser\optimization_guide\optimization_guide_keyed_service.cc:90:35
#11 0x7ff841a34083 in OptimizationGuideKeyedService::OptimizationGuideKeyedService(class content::BrowserContext *)
src\chrome\browser\optimization_guide\optimization_guide_keyed_service.cc:74:3
```

```
#12 0x7ff838e127ad in BrowserContextKeyedServiceFactory::BuildServiceInstanceFor(void *) const
src/components/keyed_service/content/browser_context_keyed_service_factory.cc:95:7
#13 0x7ff837c01f3f in KeyedServiceFactory::GetServiceForContext(void *, bool) src/components/keyed_service/core/keyed_service_factory.cc:80:15
#14 0x7ff83abe703c in DependencyManager::CreateContextServices(void *, bool) src/components/keyed_service/core/dependency_manager.cc:87:16
#15 0x7ff838e11bdc in BrowserContextDependencyManager::DoCreateBrowserContextServices(class content::BrowserContext *, bool)
src/components/keyed_service/content/browser_context_dependency_manager.cc:46:22
#16 0x7ff839983637 in ProfileImpl::OnLocaleReady(enum Profile::CreateMode) src/chrome/browser/profiles/profile_impl.cc:1099:51
#17 0x7ff83997cbb0 in ProfileImpl::OnPrefsLoaded(enum Profile::CreateMode, bool) src/chrome/browser/profiles/profile_impl.cc:1140:3
#18 0x7ff83997a032 in ProfileImpl::ProfileImpl(class base::FilePath const &, class Profile::Delegate *, enum Profile::CreateMode, class base::Time, class
scoped_refptr<class base::SequencedTaskRunner>) src/chrome/browser/profiles/profile_impl.cc:554:5
#19 0x7ff839978f2d in Profile::CreateProfile(class base::FilePath const &, class Profile::Delegate *, enum Profile::CreateMode)
src/chrome/browser/profiles/profile_impl.cc:382:59
#20 0x7ff836617cc3 in ProfileManager::CreateProfileHelper(class base::FilePath const &) src/chrome/browser/profiles/profile_manager.cc:1313:10
#21 0x7ff83660af21 in ProfileManager::CreateAndInitializeProfile(class base::FilePath const &) src/chrome/browser/profiles/profile_manager.cc:1743:38
#22 0x7ff836608150 in ProfileManager::GetProfile(class base::FilePath const &) src/chrome/browser/profiles/profile_manager.cc:737:10
#23 0x7ff83ce3799e in GetStartupProfile(class base::FilePath const &, class base::CommandLine const &)
src/chrome/browser/ui/startup/startup_browser_creator.cc:1534:39
#24 0x7ff8396c81f0 in `anonymous namespace'::CreatePrimaryProfile src/chrome/browser/chrome_browser_main.cc:415:18
#25 0x7ff8396cf4cd in ChromeBrowserMainParts::PreMainMessageLoopRunImpl(void) src/chrome/browser/chrome_browser_main.cc:1403:37
#26 0x7ff8396c3a9c in ChromeBrowserMainParts::PreMainMessageLoopRun(void) src/chrome/browser/chrome_browser_main.cc:1052:18
#27 0x7ff82e0f40ee in content::BrowserMainLoop::PreMainMessageLoopRun(void) src/content/browser/browser_main_loop.cc:938:28
```

SUMMARY: AddressSanitizer: heap-use-after-free src/content/browser/file_system_access/file_system_access_manager_impl.cc:1377:39 in content::FileSystemAccessManagerImpl::GetSharedHandleStateForPath(class base::FilePath const &, class url::Origin const &, enum content::FileSystemAccessPermissionContext::HandleType, enum content::FileSystemAccessPermissionContext::UserAction)

Shadow bytes around the buggy address:

```
0x04347c885770: fd fd fd fd fd fd fd fd fa fa fa fa fa fa
0x04347c885780: fa fa fa fa fa fa fa fa fd fd fd fd fd fd
0x04347c885790: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x04347c8857a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x04347c8857b0: fd fd fd fd fd fd fd fd fd fd fa fa fa fa
=>0x04347c8857c0: fa fa fa fa fa fa fa fa fa[fd]fd fd fd fd fd
0x04347c8857d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x04347c8857e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x04347c8857f0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
0x04347c885800: fa fa fa fa fa fa fa fa fd fd fd fd fd fd
0x04347c885810: fd fd fd fd fd fd fd fd fd fd fd fd fd fd
```

Shadow byte legend (one shadow byte represents 8 application bytes):

```
Addressable: 00
Partially addressable: 01 02 03 04 05 06 07
Heap left redzone: fa
Freed heap region: fd
Stack left redzone: f1
Stack mid redzone: f2
Stack right redzone: f3
Stack after return: f5
Stack use after scope: f8
Global redzone: f9
Global init order: f6
Poisoned by user: f7
Container overflow: fc
Array cookie: ac
Intra object redzone: bb
ASan internal: fe
Left alloca redzone: ca
Right alloca redzone: cb
==780772==ABORTING
```

CREDIT INFORMATION

Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?

Reporter credit: SorryMybad(@S0rryMybad) of Kunlun Lab

```
1.html
1.8 KB View Download

copy_mojos_bindings.py
512 bytes View Download
```

Comment 1 by sheriffbot on Thu, Sep 9, 2021, 8:22 AM EDT Project Member

Labels: external_security_report

Comment 2 by ClusterFuzz on Thu, Sep 9, 2021, 8:57 AM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5709519387426816>.

Comment 3 by ClusterFuzz on Thu, Sep 9, 2021, 2:51 PM EDT Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=5760223623839744>.

Comment 4 by adetaylor@google.com on Thu, Sep 9, 2021, 5:06 PM EDT Project Member

I can't reproduce this (using asan-linux-release-902206 on Linux x64).

It feels to me like your PoC may not be working right in my environment? Or I'm misunderstanding your instructions. The window.close() function doesn't work. Developer tools says "Scripts may close only the windows that were opened by them.". Yet from the stack traces you've provided, this looks like a profile destruction bug.

Also, the inclusion of midi_service.mojom.js appears to be unnecessary?

Comment 5 by adetaylor@google.com on Thu, Sep 9, 2021, 5:22 PM EDT Project Member

Labels: Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros

Whilst I can't reproduce this, the description of the root cause behind the UaF is very clear and meets the bar for us to pass this on beyond the security team.

Severity:

Browser process UaF, triggerable via Mojo from renderer process ==> high severity.

The stack traces provided suggest that this happens on profile destruction only. It shouldn't normally be possible for a website to cause this; the site has to induce the user to close a window (e.g. an Incognito window). Therefore we usually mitigate profile destruction bugs down by a level ==> rating this medium.

Foundin: not sure yet. Unfortunately the reporter doesn't specify the exact version they used, so I'm having a hard time matching up line numbers with their stack trace.

Comment 6 by [adetaylor@google.com](#) on Thu, Sep 9, 2021, 5:24 PM EDT Project Member

Owner: mek@chromium.org
Cc: asully@chromium.org pwnall@chromium.org
Labels: Pri-1
Components: Blink>Storage>FileSystem

Comment 7 by [mek@chromium.org](#) on Thu, Sep 9, 2021, 5:32 PM EDT Project Member

Owner: asully@chromium.org
Cc: mek@chromium.org

asully: Can you try to fix this? I think the suggested solution (of having some kind of Shutdown method called by StoragePartitionImpl that nulls out the permission context) sounds reasonable.

Comment 8 by [adetaylor@google.com](#) on Thu, Sep 9, 2021, 5:35 PM EDT Project Member

Labels: FoundIn-93

It looks to me like the fundamental ownership stuff in this code hasn't changed since 93.0.4577.63, so marking as FoundIn-93.

Comment 9 by [sheriffbot](#) on Thu, Sep 9, 2021, 5:39 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 10 by [soulc...@gmail.com](#) on Thu, Sep 9, 2021, 6:28 PM EDT

Re #c5:

The window.close() should be work, I think you misunderstanding my instructions. You need to use "out/Debug/chrome --enable-blink-features=MojoJS 127.0.0.1:8000/1.html" to open the 1.html website and 1.html is the last tab of Chromium, and window.close() should work and close all the processes.

On the other hand, from a compromised window, it is very easy to patch (please note that this is not need if you follow my instructions I said above) the related logic in "void DOMWindow::Close(LocalDOMWindow* incumbent_window)":

```
===
diff --git a/third_party/blink/renderer/core/frame/dom_window.cc b/third_party/blink/renderer/core/frame/dom_window.cc
index b52271f53c5e..46b78332a7c6 100644
--- a/third_party/blink/renderer/core/frame/dom_window.cc
+++ b/third_party/blink/renderer/core/frame/dom_window.cc
@@ -364,18 +364,7 @@ void DOMWindow::Close(LocalDOMWindow* incumbent_window) {
   bool allow_scripts_to_close_windows =
     settings && settings->GetAllowScriptsToCloseWindows();

-  if (!page->OpenedByDOM() && GetFrame()->Client()->BackForwardLength() > 1 &&
-      !allow_scripts_to_close_windows) {
-    active_document->domWindow()->GetFrameConsole()->AddMessage(
-      MakeGarbageCollected<ConsoleMessage>(
-        mojom::ConsoleMessageSource::kJavaScript,
-        mojom::ConsoleMessageLevel::kWarning,
-        "Scripts may close only the windows that were opened by them.));
-    return;
-  }
-
-  if (!GetFrame()->ShouldClose())
-    return;
+
+  ExecutionContext* execution_context = nullptr;
+  if (auto* local_dom_window = DynamicTo<LocalDOMWindow>(this)) {
===
```

So I think " It shouldn't normally be possible for a website to cause this; the site has to induce the user to close a window (e.g. an Incognito window). Therefore we usually mitigate profile destruction bugs down by a level => rating this medium." is wrong. This bug should be "Security_Severity-High".

Comment 11 by [adetaylor@google.com](#) on Thu, Sep 9, 2021, 7:39 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 12 by [adetaylor@google.com](#) on Thu, Sep 9, 2021, 8:25 PM EDT Project Member

Re #c10 - OK, I learned today that websites can self-close if they are opened from the command-line. window.close() did indeed work when the site was opened that way. Nevertheless it's not _normally_ possible for a website to close itself, so profile deletion bugs are regarded as somewhat less serious than other UaFs.

As it happens, I still can't reproduce the UaF - Chrome closes normally. But that could be timing anyway.

Comment 13 by [soulc...@gmail.com](#) on Thu, Sep 9, 2021, 10:44 PM EDT

Re #c12, so from a compromised renderer, it is easy to close itself as we can modify renderer memory and bypass this check I mention in #c10:

```
===
if (!page->OpenedByDOM() && GetFrame()->Client()->BackForwardLength() > 1 &&
    !allow_scripts_to_close_windows) {
===
```

You still consider it's not _normally_ possible for a website to close itself?

Comment 14 by [sheriffbot](#) on Fri, Sep 10, 2021, 12:52 PM EDT Project Member

Labels: Target-94 M-94

Setting milestone and target because of medium severity.

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

Comment 15 by [sheriffbot](#) on Fri, Sep 10, 2021, 2:22 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 16 by [Git Watcher](#) on Fri, Sep 10, 2021, 5:14 PM EDT Project Member

The following revision refers to this bug:
<https://chromium.googlesource.com/chromium/src/+951339b41022b08a67ad94ba5960b05c84bf4cf2>

commit 951339b41022b08a67ad94ba5960b05c84bf4cf2
Author: Austin Sullivan <asully@chromium.org>
Date: Fri Sep 10 21:13:44 2021

FSA: Fix race condition in manager

[Bug-1249030](#)

Change-Id: I1ea819d1d6ac63ec8f400a45c893da49596235ef

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3154425>

Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>

Auto-Submit: Austin Sullivan <asully@chromium.org>

Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>

Cr-Commit-Position: refs/heads/main@(#920376)

[modify] https://crrev.com/951339b41022b08a67ad94ba5960b05c84bf4cf2/content/browser/file_system_access/file_system_access_manager_impl.cc

[modify] https://crrev.com/951339b41022b08a67ad94ba5960b05c84bf4cf2/content/browser/file_system_access/file_system_access_manager_impl.h

[modify] https://crrev.com/951339b41022b08a67ad94ba5960b05c84bf4cf2/content/browser/storage_partition_impl.cc

Comment 17 by asully@chromium.org on Fri, Sep 10, 2021, 5:35 PM EDT Project Member

Status: Fixed (was: Assigned)

It looks like both myself and clusterfuzz were unable to reproduce this crash, but the change which just landed should have fixed it.

@OP: Once this change hits Canary, can you confirm this bug no longer reproduces? (You can check which release this change is in here:

<https://chromiumdash.appspot.com/commit/951339b41022b08a67ad94ba5960b05c84bf4cf2>)

Comment 18 by sheriffbot on Sat, Sep 11, 2021, 12:46 PM EDT Project Member

Labels: reward-topanel

Comment 19 by sheriffbot on Sat, Sep 11, 2021, 1:45 PM EDT Project Member

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

Comment 20 by sheriffbot on Sat, Sep 11, 2021, 2:10 PM EDT Project Member

Labels: Merge-Request-94 Merge-Request-95

Requesting merge to beta M94 because latest trunk commit (920376) appears to be after beta branch point (911515).

Requesting merge to dev M95 because latest trunk commit (920376) appears to be after dev branch point (920003).

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

Comment 21 by sheriffbot on Sat, Sep 11, 2021, 2:16 PM EDT Project Member

Labels: -Merge-Request-94 Merge-Review-94 Hotlist-Merge-Review

This bug requires manual review: We are only 9 days from stable.

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/+main/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: govind@ (Android), harrysouders@ (iOS), matthewjoseph@ (ChromeOS), srinivassista@ (Desktop)

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

Comment 22 by sheriffbot on Sun, Sep 12, 2021, 2:16 PM EDT Project Member

Labels: -Merge-Request-95 Hotlist-Merge-Approved Merge-Approved-95

Your change meets the bar and is auto-approved for M95. Please go ahead and merge the CL to branch 4638 (refs/branch-heads/4638) manually. Please contact milestone owner if you have questions.

Merge instructions: <https://www.chromium.org/developers/how-tos/drover>

Owners: benmason@ (Android), harrysouders@ (iOS), None@ (ChromeOS), pbommana@ (Desktop)

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

Comment 23 by srinivassista@google.com on Mon, Sep 13, 2021, 12:17 PM EDT Project Member

has this been verified on canary? , can you pls answer [comment #21](#) for merge review.

Comment 24 by pbommana@google.com on Mon, Sep 13, 2021, 1:20 PM EDT Project Member

Your change has been approved for M95. Please go ahead and merge the CL to branch 4638 manually asap so that it would be part of this week's Dev release i.e., tomorrow.

Comment 25 by pbommana@google.com on Mon, Sep 13, 2021, 1:21 PM EDT Project Member

Your change has been approved for M95. Please go ahead and merge the CL to branch 4638 manually asap so that it would be part of this week's Dev release i.e., tomorrow.

Comment 26 by Git Watcher on Mon, Sep 13, 2021, 7:20 PM EDT Project Member

Labels: -merge-approved-95 merge-merged-4638 merge-merged-95

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+bfc77020c6ffcaf5216577ba2e5dc7344d0f5fd6>

commit [bfc77020c6ffcaf5216577ba2e5dc7344d0f5fd6](https://chromium.googlesource.com/chromium/src/+bfc77020c6ffcaf5216577ba2e5dc7344d0f5fd6)

Author: Austin Sullivan <asully@chromium.org>

Date: Mon Sep 13 23:19:52 2021

FSA: Fix race condition in manager

(cherry picked from commit [951339b41022b08a67ad94ba5960b05c84bf4cf2](https://chromium.googlesource.com/chromium/src/+bfc77020c6ffcaf5216577ba2e5dc7344d0f5fd6))

[Bug-1249030](#)

Change-Id: I1ea819d1d6ac63ec8f400a45c893da49596235ef

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3154425>

Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>

Auto-Submit: Austin Sullivan <asully@chromium.org>

Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@(#920376)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3158788>

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

Cr-Commit-Position: refs/branch-heads/4638@{#26}
Cr-Branched-From: 159257cab5585bc8421abf347984bb32fde9eb9-refs/heads/main@{#920003}

[modify] https://crrev.com/bfc77020c8ffca5216577ba2e5dc7344d0f5fd6/content/browser/file_system_access/file_system_access_manager_impl.cc
[modify] https://crrev.com/bfc77020c8ffca5216577ba2e5dc7344d0f5fd6/content/browser/file_system_access/file_system_access_manager_impl.h
[modify] https://crrev.com/bfc77020c8ffca5216577ba2e5dc7344d0f5fd6/content/browser/storage_partition_impl.cc

Comment 27 by [srinivassista@google.com](#) on Tue, Sep 14, 2021, 12:55 PM EDT Project Member

since this is hard to repro and we are cutting stable RC for m94 today, we will wait for the reporter to confirm this is working as intended before we take merge to M94 and include in first re-spin

Comment 28 by [soulc...@gmail.com](#) on Tue, Sep 14, 2021, 11:28 PM EDT

Re [c#27](#):

Yes, good fix.

Comment 29 by [srinivassista@google.com](#) on Wed, Sep 15, 2021, 12:12 PM EDT Project Member

Labels: -Merge-Review-94 Merge-Approved-94

Merge approved for m94 branch:4606 (We will take in next M94 release)

Comment 30 by [Git Watcher](#) on Wed, Sep 15, 2021, 7:58 PM EDT Project Member

Labels: -merge-approved-94 merge-merged-4606 merge-merged-94

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+4e528a5a8d839f8b382d25821a2807546f97d2cc>

commit [4e528a5a8d839f8b382d25821a2807546f97d2cc](#)

Author: Austin Sullivan <asully@chromium.org>

Date: Wed Sep 15 23:57:27 2021

FSA: Fix race condition in manager

(cherry picked from commit [951339b41022b08a67ad94ba5960b05c84b4cf2](#))

[Bug-1249030](#)

Change-Id: I1ea819d1d6ac63ec8f400a45c893da49596235ef

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3154425>

Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>

Auto-Submit: Austin Sullivan <asully@chromium.org>

Reviewed-by: Marijn Kruisselbrink <mek@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#920376}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3160301>

Commit-Queue: Austin Sullivan <asully@chromium.org>

Cr-Commit-Position: refs/branch-heads/4606@{#1077}

Cr-Branched-From: 35b0d5a9dc8362adfd44e2614f0d5b7402ef63d0-refs/heads/master@{#911515}

[modify] https://crrev.com/4e528a5a8d839f8b382d25821a2807546f97d2cc/content/browser/file_system_access/file_system_access_manager_impl.cc

[modify] https://crrev.com/4e528a5a8d839f8b382d25821a2807546f97d2cc/content/browser/file_system_access/file_system_access_manager_impl.h

[modify] https://crrev.com/4e528a5a8d839f8b382d25821a2807546f97d2cc/content/browser/storage_partition_impl.cc

Comment 31 by [amyressler@chromium.org](#) on Mon, Sep 20, 2021, 5:55 PM EDT Project Member

Labels: Release-0-M94

Comment 32 by [amyressler@google.com](#) on Tue, Sep 21, 2021, 1:19 PM EDT Project Member

Labels: CVE-2021-37970 CVE_description-missing

Comment 33 by [rzanoni@google.com](#) on Tue, Sep 28, 2021, 8:09 AM EDT Project Member

Labels: LTS-Security-90 LTS-Size-Small LTS-Complexity-Trivial LTS-Merge-Request-90

Comment 34 by [gianluca@google.com](#) on Tue, Sep 28, 2021, 10:58 AM EDT Project Member

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 35 by [Git Watcher](#) on Wed, Sep 29, 2021, 4:21 AM EDT Project Member

Labels: merge-merged-4430

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src/+f703dacd1a1d9a80cd7486cdb1936f11ef8138a5>

commit [f703dacd1a1d9a80cd7486cdb1936f11ef8138a5](#)

Author: Austin Sullivan <asully@chromium.org>

Date: Wed Sep 29 08:20:51 2021

[M90-LTS] FSA: Fix race condition in manager

(cherry picked from commit [951339b41022b08a67ad94ba5960b05c84b4cf2](#))

[Bug-1249030](#)

Change-Id: I1ea819d1d6ac63ec8f400a45c893da49596235ef

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3154425>

Commit-Queue: Marijn Kruisselbrink <mek@chromium.org>

Auto-Submit: Austin Sullivan <asully@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#920376}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+3182123>

Reviewed-by: Austin Sullivan <asully@chromium.org>

Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>

Owners-Override: Victor-Gabriel Savu <vsavu@google.com>

Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>

Cr-Commit-Position: refs/branch-heads/4430@{#1624}

Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/f703dacd1a1d9a80cd7486cdb1936f11ef8138a5/content/browser/file_system_access/file_system_access_manager_impl.h

[modify] https://crrev.com/f703dacd1a1d9a80cd7486cdb1936f11ef8138a5/content/browser/storage_partition_impl.cc

[modify] https://crrev.com/f703dacd1a1d9a80cd7486cdb1936f11ef8138a5/content/browser/file_system_access/file_system_access_manager_impl.cc

Comment 36 by [rzanoni@google.com](#) on Wed, Sep 29, 2021, 4:46 AM EDT Project Member

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 37 by [soulc...@gmail.com](#) on Wed, Oct 6, 2021, 12:43 AM EDT

Hi, any update of bounty?

[Comment 38](#) by amyressler@google.com on Fri, Oct 8, 2021, 5:31 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

[Comment 39](#) by soulc...@gmail.com on Sun, Oct 10, 2021, 9:30 PM EDT

c#38

Any update for bounty?

[Comment 40](#) by amyressler@google.com on Wed, Oct 13, 2021, 7:16 PM EDT 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 41](#) by amyressler@chromium.org on Wed, Oct 13, 2021, 7:39 PM EDT Project Member

Congratulations - the VRP Panel has decided to award you \$15,000 for this report! Thank you for your efforts and nice finding!

[Comment 42](#) by amyressler@google.com on Thu, Oct 14, 2021, 7:10 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

[Comment 43](#) by [sheriffbot](#) on Sun, Dec 19, 2021, 1:28 PM EST Project Member

Labels: -Restrict-View-SecurityNotify allpublic

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

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