☆ Starred by 3 users

Owner:	sa...@chromium.org
CC:	solomonkinard@chromium.org tjudkins@chromium.org
Status:	Fixed *(Closed)*
Components:	Platform>Extensions>API
Modified:	Nov 8, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
M-92
Target-92
external_security_report
merge-merged-4430
merge-merged-90
FoundIn-92
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
LTS-Size-Small
LTS-Complexity-Minimal
Release-2-M92
CVE-2021-30601
merge-merged-4515_132

Issue 1234009: Use-after-Free in FileSystemChooseEntryFunction::FilesSelected

Reported by etern...@gmail.com on Wed, Jul 28, 2021, 11:59 AM EDT

Code

Report description

Use-after-Free in FileSystemChooseEntryFunction::FilesSelected

---

Bug location

Which product or website have you found a vulnerability in?

Google Chrome

The problem

Please describe the technical details of the vulnerability

Use-after-Free in FileSystemChooseEntryFunction::FilesSelected
Root Cause and some notes
The `web_contents` is posted to a separate sequence[0] and `web_contents` may be destroyed in UI by the time it runs,When it post webcontents back[1] from a seperate sequence and use it in[2],UAF happens.

[0]https://source.chromium.org/chromium/chromium/src/+/main:extensions/browser/api/file_system/file_system_api.cc;l=537?q=file_system_api
[1]https://source.chromium.org/chromium/chromium/src/+/main:extensions/browser/api/file_system/file_system_api.cc;l=580;drc=80def040657db16e79f59e7e3b27857014c0f58d?q=file_system_api
[2]https://source.chromium.org/chromium/chromium/src/+/main:components/constrained_window/constrained_window_views.cc;l=167;drc=80def040657db16e79f59e7e3b27857014c0f58d;bpv=0;bpt=1

https://chromium-review.googlesource.com/c/chromium/src/+/3041006
The pattern of this vulnerability is similar to this patch.

Reproduce
0. patch the sleep as following
  (The patch is not necessary,just make it trigger stable)

```cpp
void FileSystemChooseEntryFunction::ConfirmDirectoryAccessAsync(
    bool non_native_path,
    const std::vector<base::FilePath>& paths,
    content::WebContents* web_contents) {
[+]    sleep(2);
  const base::FilePath check_path =
      non_native_path ? paths[0] : base::MakeAbsoluteFilePath(paths[0]);
  if (check_path.empty()) {
    content::GetUIThreadTaskRunner({})->PostTask(
        FROM_HERE,
        base::BindOnce(&FileSystemChooseEntryFunction::FileSelectionCanceled,
                       this));
      LOG(ERROR) << "path empty";
      return;
  }
```

1. run the app
2. choose your root user directory and wait for the crash

UAF log

```
==7287==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e00022ec80 at pc 0x000116689839 bp 0x7ffee4cb4810 sp 0x7ffee4cb4808
READ of size 8 at 0x61e00022ec80 thread T0
    #0 0x116689838 in TabModalConfirmDialogDelegate::TabModalConfirmDialogDelegate(content::WebContents*) tab_modal_confirm_dialog_delegate.cc:21
    #1 0x1164541cf in CreateDirectoryAccessConfirmationDialog(bool, std::__Cr::basic_string<char16_t, std::__Cr::char_traits<char16_t>, std::__Cr::allocator<char16_t> >
const&, content::WebContents*, base::OnceCallback<void ()>, base::OnceCallback<void ()>) directory_access_confirmation_dialog.cc:99
    #2 0x115133d56 in extensions::ChromeFileSystemDelegate::ConfirmSensitiveDirectoryAccess(bool, std::__Cr::basic_string<char16_t, std::__Cr::char_traits<char16_t>,
std::__Cr::allocator<char16_t> > const&, content::WebContents*, base::OnceCallback<void ()>, base::OnceCallback<void ()>) chrome_file_system_delegate.cc:304
    #3 0x1104530f9 in extensions::FileSystemChooseEntryFunction::ConfirmSensitiveDirectoryAccess(std::__Cr::vector<base::FilePath, std::__Cr::allocator<base::FilePath> >
const&, content::WebContents*) file_system_api.cc:611
    #4 0x10be27719 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) task_annotator.cc:178
    #5 0x10be70736 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:360
    #6 0x10be6fe13 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:260
    #7 0x10be712a1 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc
    #8 0x10bf96458 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:384
    #9 0x10bf7dbe9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (libbase.dylib:x86_64+0x372be9)
    #10 0x10bf94c75 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:360
    #11 0x7fff20480a0b in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64h+0x81a0b)
    #12 0x7fff20480973 in __CFRunLoopDoSource0+0xb3 (CoreFoundation:x86_64h+0x81973)
    #13 0x7fff204806ee in __CFRunLoopDoSources0+0xf7 (CoreFoundation:x86_64h+0x816ee)
    #14 0x7fff2047f120 in __CFRunLoopRun+0x379 (CoreFoundation:x86_64h+0x80120)
    #15 0x7fff2047e6cd in CFRunLoopRunSpecific+0x232 (CoreFoundation:x86_64h+0x7f6cd)
    #16 0x7fff2870662f in RunCurrentEventLoopInMode+0x123 (HIToolbox:x86_64+0x3162f)
    #17 0x7fff2870642b in ReceiveNextEventCommon+0x2c4 (HIToolbox:x86_64+0x3142b)
    #18 0x7fff2870614e in _BlockUntilNextEventMatchingListInModeWithFilter+0x3f (HIToolbox:x86_64+0x3114e)
    #19 0x7fff22c9e9b0 in _DPSNextEvent+0x372 (AppKit:x86_64+0x3e9b0)
    #20 0x7fff22c9d176 in -[NSApplication(NSEvent) _nextEventMatchingEventMask:untilDate:inMode:dequeue:]+0x555 (AppKit:x86_64+0x3d176)
    #21 0x1127c4782 in __71-[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke chrome_browser_application_mac.mm:237
    #22 0x10bf7dbe9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (libbase.dylib:x86_64+0x372be9)
    #23 0x1127c431a in -[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:] chrome_browser_application_mac.mm:236
    #24 0x7fff22c8f689 in -[NSApplication run]+0x249 (AppKit:x86_64+0x2f689)
    #25 0x10bf98b4a in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*) message_pump_mac.mm:729
    #26 0x10bf938d8 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*) message_pump_mac.mm:157
    #27 0x10be71995 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
thread_controller_with_message_pump_impl.cc:467
    #28 0x10bd7903e in base::RunLoop::Run(base::Location const&) run_loop.cc:134
    #29 0x1277a8455 in content::BrowserMainLoop::RunMainMessageLoop() browser_main_loop.cc:999
    #30 0x1277acc91 in content::BrowserMainRunnerImpl::Run() browser_main_runner_impl.cc:152
    #31 0x1277a1b9c in content::BrowserMain(content::MainFunctionParams const&) browser_main.cc:47
    #32 0x12989283c in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content_main_runner_impl.cc:1080
    #33 0x129891af9 in content::ContentMainRunnerImpl::Run(bool) content_main_runner_impl.cc:955
    #34 0x12988ea76 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content_main.cc:386
    #35 0x12988f07c in content::ContentMain(content::ContentMainParams const&) content_main.cc:412
    #36 0x10f626845 in ChromeMain chrome_main.cc:151
    #37 0x10af4a88f in main chrome_exe_main_mac.cc:114
    #38 0x7fff203a3620 in start+0x0 (libdyld.dylib:x86_64+0x15620)

0x61e00022ec80 is located 0 bytes inside of 2712-byte region [0x61e00022ec80,0x61e00022f718)
freed by thread T0 here:
    #0 0x10b2f10bd  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x520bd)
    #1 0x110011a73 in extensions::AppWindowContentsImpl::~AppWindowContentsImpl() app_window_contents.cc:27
    #2 0x11000912d in extensions::AppWindow::~AppWindow() app_window.cc:339
    #3 0x1100093ed in extensions::AppWindow::~AppWindow() app_window.cc:337
    #4 0x11000b002 in extensions::AppWindow::OnNativeClose() app_window.cc:503
    #5 0x1353af768 in views::Widget::OnNativeWidgetDestroyed() widget.cc:1298
    #6 0x135438881 in views::NativeWidgetMac::WindowDestroyed() native_widget_mac.mm:142
    #7 0x1377a8cbb in -[ViewsNSWindowDelegate windowWillClose:] views_nswindow_delegate.mm:182
    #8 0x7fff20475feb in __CFNOTIFICATIONCENTER_IS_CALLING_OUT_TO_AN_OBSERVER__+0xb (CoreFoundation:x86_64h+0x76feb)
    #9 0x7fff2051189a in ___CFXRegistrationPost_block_invoke+0x30 (CoreFoundation:x86_64h+0x11289a)
    #10 0x7fff2051180e in _CFXRegistrationPost+0x1c5 (CoreFoundation:x86_64h+0x11280e)
    #11 0x7fff20446bdd in _CFXNotificationPost+0x2d2 (CoreFoundation:x86_64h+0x47bdd)
    #12 0x7fff211b5abd in -[NSNotificationCenter postNotificationName:object:userInfo:]+0x3a (Foundation:x86_64+0x9abd)
    #13 0x7fff2354cb91 in -[NSWindow _finishClosingWindow]+0x7b (AppKit:x86_64+0x8ecb91)
    #14 0x7fff22fe2b0e in -[NSWindow _close]+0x15a (AppKit:x86_64+0x382b0e)
    #15 0x13779d880 in base::internal::Invoker<base::internal::BindState<base::ScopedTypeRef<void () block_pointer, base::mac::internal::ScopedBlockTraits<void ()
block_pointer> > >, void ()>::RunOnce(base::internal::BindStateBase*) bind_internal.h:690
    #16 0x10be27719 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) task_annotator.cc:178
    #17 0x10be70736 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:360
    #18 0x10be6fe13 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:260
    #19 0x10be712a1 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc
    #20 0x10bf96458 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:384
    #21 0x10bf7dbe9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (libbase.dylib:x86_64+0x372be9)
    #22 0x10bf94c75 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:360
    #23 0x7fff20480a0b in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64h+0x81a0b)
    #24 0x7fff20480973 in __CFRunLoopDoSource0+0xb3 (CoreFoundation:x86_64h+0x81973)
    #25 0x7fff204806ee in __CFRunLoopDoSources0+0xf7 (CoreFoundation:x86_64h+0x816ee)
    #26 0x7fff2047f120 in __CFRunLoopRun+0x379 (CoreFoundation:x86_64h+0x80120)
    #27 0x7fff2047e6cd in CFRunLoopRunSpecific+0x232 (CoreFoundation:x86_64h+0x7f6cd)
    #28 0x7fff2870662f in RunCurrentEventLoopInMode+0x123 (HIToolbox:x86_64+0x3162f)
    #29 0x7fff2870642b in ReceiveNextEventCommon+0x2c4 (HIToolbox:x86_64+0x3142b)

previously allocated by thread T0 here:
    #0 0x10b2f0c9d  (libclang_rt.asan_osx_dynamic.dylib:x86_64+0x51c9d)
    #1 0x128a4500b in content::WebContentsImpl::CreateWithOpener(content::WebContents::CreateParams const&, content::RenderFrameHostImpl*)
web_contents_impl.cc:1061
    #2 0x110011e1a in extensions::AppWindowContentsImpl::Initialize(content::BrowserContext*, content::RenderFrameHost*, GURL const&) app_window_contents.cc:38
    #3 0x110005fbd in extensions::AppWindow::Init(GURL const&, extensions::AppWindowContents*, content::RenderFrameHost*, extensions::AppWindow::CreateParams
const&) app_window.cc:260
    #4 0x11038d7ba in extensions::AppWindowCreateFunction::Run() app_window_api.cc:406
    #5 0x110094d67 in ExtensionFunction::RunWithValidation() extension_function.cc:513
    #6 0x11009df28 in extensions::ExtensionFunctionDispatcher::DispatchWithCallbackInternal(extensions::mojom::RequestParams const&, content::RenderFrameHost*, int,
base::OnceCallback<void (ExtensionFunction::ResponseType, base::Value const&, std::__Cr::basic_string<char, std::__Cr::char_traits<char>, std::__Cr::allocator<char> >
const&)>) extension_function_dispatcher.cc:395
    #7 0x11009d2c6 in extensions::ExtensionFunctionDispatcher::Dispatch(mojo::StructPtr<extensions::mojom::RequestParams>, content::RenderFrameHost*, int,
base::OnceCallback<void (bool, base::Value, std::__Cr::basic_string<char, std::__Cr::char_traits<char>, std::__Cr::allocator<char> > const&)>)
extension_function_dispatcher.cc:257
    #8 0x11009170a in extensions::ExtensionFrameHost::Request(mojo::StructPtr<extensions::mojom::RequestParams>, base::OnceCallback<void (bool, base::Value,
std::__Cr::basic_string<char, std::__Cr::char_traits<char>, std::__Cr::allocator<char> > const&)>) extension_frame_host.cc:40
    #9 0x10f882e9b in extensions::mojom::LocalFrameHostStubDispatch::AcceptWithResponder(extensions::mojom::LocalFrameHost*, mojo::Message*,
std::__Cr::unique_ptr<mojo::MessageReceiverWithStatus, std::__Cr::default_delete<mojo::MessageReceiverWithStatus> >) frame.mojom.cc:2204
    #10 0x10d67eb5b in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*) interface_endpoint_client.cc:829
    #11 0x10d68f9ee in mojo::MessageDispatcher::Accept(mojo::Message*) message_dispatcher.cc:48
    #12 0x10d682e2e in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*) interface_endpoint_client.cc:653
    #13 0x12147db1c in IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptOnProxyThread(mojo::Message) ipc_mojo_bootstrap.cc:950
    #14 0x12147660d in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)(mojo::Message),
scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>, void ()>::RunOnce(base::internal::BindStateBase*) bind_internal.h:690
    #15 0x10be27719 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) task_annotator.cc:178
    #16 0x10be70736 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
thread_controller_with_message_pump_impl.cc:360
    #17 0x10be6fe13 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork() thread_controller_with_message_pump_impl.cc:260
    #18 0x10be712a1 in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
thread_controller_with_message_pump_impl.cc
    #19 0x10bf96458 in base::MessagePumpCFRunLoopBase::RunWork() message_pump_mac.mm:384
    #20 0x10bf7dbe9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (libbase.dylib:x86_64+0x372be9)
    #21 0x10bf94c75 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*) message_pump_mac.mm:360
    #22 0x7fff20480a0b in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10 (CoreFoundation:x86_64h+0x81a0b)
    #23 0x7fff20480973 in __CFRunLoopDoSource0+0xb3 (CoreFoundation:x86_64h+0x81973)
    #24 0x7fff204806ee in __CFRunLoopDoSources0+0xf7 (CoreFoundation:x86_64h+0x816ee)
    #25 0x7fff2047f120 in __CFRunLoopRun+0x379 (CoreFoundation:x86_64h+0x80120)
    #26 0x7fff2047e6cd in CFRunLoopRunSpecific+0x232 (CoreFoundation:x86_64h+0x7f6cd)
    #27 0x7fff2870662f in RunCurrentEventLoopInMode+0x123 (HIToolbox:x86_64+0x3162f)
    #28 0x7fff2870642b in ReceiveNextEventCommon+0x2c4 (HIToolbox:x86_64+0x3142b)
    #29 0x7fff2870614e in _BlockUntilNextEventMatchingListInModeWithFilter+0x3f (HIToolbox:x86_64+0x3114e)

SUMMARY: AddressSanitizer: heap-use-after-free tab_modal_confirm_dialog_delegate.cc:21 in
TabModalConfirmDialogDelegate::TabModalConfirmDialogDelegate(content::WebContents*)
Shadow bytes around the buggy address:
  0x1c3c00045d40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045d50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045d60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045d70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x1c3c00045d80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x1c3c00045d90:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045da0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045db0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045dc0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045dd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x1c3c00045de0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==7287==ABORTING
```

Please briefly explain who can exploit the vulnerability, and what they gain when doing so

This vulnerability can be used for sandbox escape, because the vulnerability is in the browser process, not in the render.

The cause

What version of Chrome have you found the security issue in?

[92.0.4515.107+] + [stable]

Is the security issue related to a crash?

Yes

Choose the type of vulnerability

Sandbox Escape

Please provide your credit information

koocola(@alo_cook) and Nan Wang(@eternalsakura13) of 360 Alpha Lab

Comment 1 by etern...@gmail.com on Wed, Jul 28, 2021, 11:59 AM EDT

poc.zip
3.5 KB Download

uaf1.mp4
1.2 MB View Download

Comment 2 by chrom...@appspot.gserviceaccount.com on Wed, Jul 28, 2021, 11:59 AM EDT

Labels: external_security_report

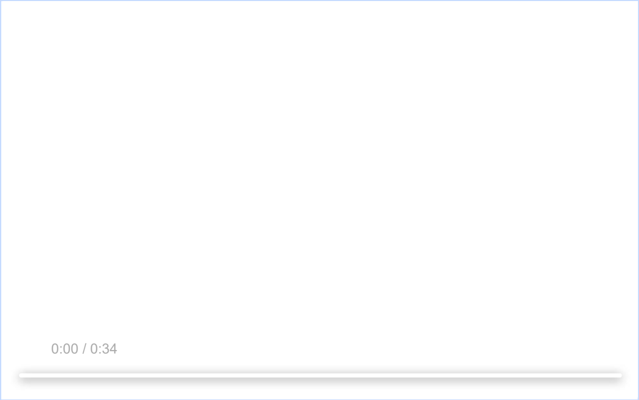
Comment 3 by etern...@gmail.com on Wed, Jul 28, 2021, 12:06 PM EDT

It should be noted that this sleep is not necessary, just because of the need for conditional competition.
If sleep is not added to my machine, the success rate is probably 10%.

Comment 4 by etern...@gmail.com on Thu, Jul 29, 2021, 1:58 AM EDT

I have provided another video for you to reproduce on ubuntu. Remember to finally select the home directory and click open.
If you have any questions, please feel free to contact me.

uaf1.mp4
4.5 MB View Download



Comment 5 Deleted

Comment 6 by mea...@chromium.org on Fri, Jul 30, 2021, 7:13 AM EDT

Status: Assigned (was: Unconfirmed)
Owner: sa...@chromium.org
Labels: Security_Severity-High Security_Impact-Stable FoundIn-92 OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-1
Components: Platform>Extensions>API

sammc: Could you please take a look?

Assigning high severity since exploitation requires an extension install.

Comment 7 by sheriffbot on Fri, Jul 30, 2021, 12:47 PM EDT

Labels: M-92 Target-92

Setting milestone and target because of high severity.

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

Comment 8 by sa...@chromium.org on Sun, Aug 1, 2021, 9:17 PM EDT

Status: Started (was: Assigned)

Comment 9 by sa...@chromium.org on Mon, Aug 2, 2021, 1:04 AM EDT

https://crrev.com/c/3063743

Comment 10 by Git Watcher on Mon, Aug 2, 2021, 3:11 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/18236a0db8341302120c60781ae3129e94fbaf1c

commit 18236a0db8341302120c60781ae3129e94fbaf1c
Author: Sam McNally <sammc@chromium.org>
Date: Mon Aug 02 07:10:35 2021

Defer looking up the WebContents for the directory confirmation dialog.

Look up the WebContents to use for the sensitive directory confirmation
dialog immediately before it's used instead of before performing some
blocking file access to determine whether it's necessary.

~~Bug: 1234009~~
Change-Id: I5e00c7fa199b3da522e1fdb73242891d7f5f7423
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3063743
Reviewed-by: Alex Danilo <adanilo@chromium.org>
Reviewed-by: Ben Wells <benwells@chromium.org>
Commit-Queue: Sam McNally <sammc@chromium.org>
Cr-Commit-Position: refs/heads/master@{#907467}

[modify] https://crrev.com/18236a0db8341302120c60781ae3129e94fbaf1c/extensions/browser/api/file_system/file_system_api.cc
[modify] https://crrev.com/18236a0db8341302120c60781ae3129e94fbaf1c/extensions/browser/api/file_system/file_system_api.h

Comment 11 by sa...@chromium.org on Mon, Aug 2, 2021, 9:15 AM EDT

Status: Fixed (was: Started)

Comment 12 by sheriffbot on Mon, Aug 2, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 13 by sheriffbot on Mon, Aug 2, 2021, 1:42 PM EDT

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

Comment 14 by sheriffbot on Mon, Aug 2, 2021, 2:07 PM EDT

Labels: Merge-Request-92 Merge-Request-93

Requesting merge to stable M92 because latest trunk commit (907467) appears to be after stable branch point (885287).

Requesting merge to beta M93 because latest trunk commit (907467) appears to be after beta branch point (902210).

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

Comment 15 by amyressler@chromium.org on Mon, Aug 2, 2021, 2:49 PM EDT

Since this fix just landed today, I'm going to decline merge approval today since we are cutting an M93 beta release tomorrow and it seems like it would be beneficial for this fix to have a bit more bake time on Canary. I will revisit in a couple of days for merge to both appropriate branches. Thanks!

Comment 16 by sheriffbot on Tue, Aug 3, 2021, 3:13 AM EDT

Labels: -Merge-Request-93 Hotlist-Merge-Review Merge-Review-93

This bug requires manual review: M93'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/+/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: benmason@(Android), govind@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 17 by ajgo@google.com on Wed, Aug 4, 2021, 6:13 PM EDT

(unzipping)

background.js
211 bytes View Download

foreground.js
133 bytes View Download

index.html
187 bytes View Download

index1.html
369 bytes View Download

manifest.json
303 bytes View Download

Comment 18 by amyressler@google.com on Wed, Aug 4, 2021, 7:08 PM EDT

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 19 by amyressler@chromium.org on Wed, Aug 4, 2021, 7:13 PM EDT

Congratulations, koocola and Nan Wang! The VRP Panel has decided to award you $20,000 for this report. Excellent work!

Comment 20 by amyressler@google.com on Fri, Aug 6, 2021, 12:27 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 21 by amyressler@google.com on Mon, Aug 9, 2021, 10:23 AM EDT

Labels: -Merge-Request-92 -Merge-Review-93 Merge-Approved-93 Merge-Approved-92

sammc@, if you are okay with the performance of this fix on Canary and there's no stability issues, please go ahead and merge to M92 (branch 4515) and M93 (branch 4577) asap. Please ensure fix is merged to M93, branch 4577, by EOD Tuesday, 10 August so it can be included in the M93 stable cut for release next week. Thanks!

Comment 22 by Git Watcher on Mon, Aug 9, 2021, 9:38 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c06871d5065b20777ab7e962f61e1d29f70cc3bc

commit c06871d5065b20777ab7e962f61e1d29f70cc3bc
Author: Sam McNally <sammc@chromium.org>
Date: Tue Aug 10 01:37:34 2021

Defer looking up the WebContents for the directory confirmation dialog.

Look up the WebContents to use for the sensitive directory confirmation
dialog immediately before it's used instead of before performing some
blocking file access to determine whether it's necessary.

(cherry picked from commit 18236a0db8341302120c60781ae3129e94fbaf1c)

~~Bug: 1234009~~
Change-Id: I5e00c7fa199b3da522e1fdb73242891d7f5f7423
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3063743
Reviewed-by: Alex Danilo <adanilo@chromium.org>
Reviewed-by: Ben Wells <benwells@chromium.org>
Commit-Queue: Sam McNally <sammc@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#907467}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3083763
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4515@{#2012}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/c06871d5065b20777ab7e962f61e1d29f70cc3bc/extensions/browser/api/file_system/file_system_api.cc
[modify] https://crrev.com/c06871d5065b20777ab7e962f61e1d29f70cc3bc/extensions/browser/api/file_system/file_system_api.h

Comment 23 by Git Watcher on Mon, Aug 9, 2021, 10:15 PM EDT

Labels: -merge-approved-93 merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/85c16cd71b8e2ea1de3c95c3b76caf86ac8d6474

commit 85c16cd71b8e2ea1de3c95c3b76caf86ac8d6474
Author: Sam McNally <sammc@chromium.org>
Date: Tue Aug 10 02:14:43 2021

Defer looking up the WebContents for the directory confirmation dialog.

Look up the WebContents to use for the sensitive directory confirmation
dialog immediately before it's used instead of before performing some
blocking file access to determine whether it's necessary.

(cherry picked from commit 18236a0db8341302120c60781ae3129e94fbaf1c)

~~Bug: 1234009~~
Change-Id: I5e00c7fa199b3da522e1fdb73242891d7f5f7423
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3063743
Reviewed-by: Alex Danilo <adanilo@chromium.org>
Reviewed-by: Ben Wells <benwells@chromium.org>
Commit-Queue: Sam McNally <sammc@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#907467}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3083204
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4577@{#648}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/85c16cd71b8e2ea1de3c95c3b76caf86ac8d6474/extensions/browser/api/file_system/file_system_api.cc
[modify] https://crrev.com/85c16cd71b8e2ea1de3c95c3b76caf86ac8d6474/extensions/browser/api/file_system/file_system_api.h

Comment 24 by amyressler@google.com on Mon, Aug 16, 2021, 10:11 AM EDT

Labels: Release-2-M92

Comment 25 by amyressler@google.com on Mon, Aug 16, 2021, 10:20 AM EDT

Labels: CVE-2021-30601 CVE_description-missing

Comment 26 by rzanoni@google.com on Tue, Aug 17, 2021, 8:12 AM EDT

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 27 by rzanoni@google.com on Thu, Aug 19, 2021, 11:32 AM EDT

Labels: LTS-Size-Small LTS-Complexity-Minimal

Comment 28 by gianluca@google.com on Fri, Aug 20, 2021, 3:31 AM EDT

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

Comment 29 by Git Watcher on Fri, Aug 20, 2021, 1:22 PM EDT

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d8f7a221d014da2d7b5a055c98a1e9acf418af32

commit d8f7a221d014da2d7b5a055c98a1e9acf418af32

Author: Sam McNally <sammc@chromium.org>
Date: Fri Aug 20 17:21:48 2021

[M90-LTS] Defer looking up the WebContents for the directory confirmation dialog.

Look up the WebContents to use for the sensitive directory confirmation
dialog immediately before it's used instead of before performing some
blocking file access to determine whether it's necessary.

(cherry picked from commit 18236a0db8341302120c60781ae3129e94fbaf1c)

~~Bug: 1234009~~
Change-Id: I5e00c7fa199b3da522e1fdb73242891d7f5f7423
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3063743
Commit-Queue: Sam McNally <sammc@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#907467}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3097732
Reviewed-by: Sam McNally <sammc@chromium.org>
Reviewed-by: Jana Grill <janagrill@google.com>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1569}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/d8f7a221d014da2d7b5a055c98a1e9acf418af32/extensions/browser/api/file_system/file_system_api.cc
[modify] https://crrev.com/d8f7a221d014da2d7b5a055c98a1e9acf418af32/extensions/browser/api/file_system/file_system_api.h

Comment 30 by rzanoni@google.com on Mon, Aug 23, 2021, 4:07 AM EDT

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

Comment 31 by amyressler@google.com on Thu, Aug 26, 2021, 1:44 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by Git Watcher on Mon, Sep 20, 2021, 10:00 PM EDT

Labels: merge-merged-4515_132

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c5f9c40e9b106704130ffb8789ac68693152aedd

commit c5f9c40e9b106704130ffb8789ac68693152aedd
Author: Sam McNally <sammc@chromium.org>
Date: Tue Sep 21 01:59:41 2021

Defer looking up the WebContents for the directory confirmation dialog.

Look up the WebContents to use for the sensitive directory confirmation
dialog immediately before it's used instead of before performing some
blocking file access to determine whether it's necessary.

(cherry picked from commit 18236a0db8341302120c60781ae3129e94fbaf1c)

(cherry picked from commit c06871d5065b20777ab7e962f61e1d29f70cc3bc)

~~Bug: 1234009~~
Change-Id: I5e00c7fa199b3da522e1fdb73242891d7f5f7423
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3063743
Reviewed-by: Alex Danilo <adanilo@chromium.org>
Reviewed-by: Ben Wells <benwells@chromium.org>
Commit-Queue: Sam McNally <sammc@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#907467}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3083763
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Original-Commit-Position: refs/branch-heads/4515@{#2012}
Cr-Original-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3171856
Auto-Submit: Joe Tessler <jrt@chromium.org>
Reviewed-by: Sam McNally <sammc@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515_132@{#5}
Cr-Branched-From: 8e089f9dc0d240f50afd19b527a90447b90ca5bb-refs/branch-heads/4515@{#1934}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/c5f9c40e9b106704130ffb8789ac68693152aedd/extensions/browser/api/file_system/file_system_api.h
[modify] https://crrev.com/c5f9c40e9b106704130ffb8789ac68693152aedd/extensions/browser/api/file_system/file_system_api.cc

Comment 33 by sheriffbot on Mon, Nov 8, 2021, 1:31 PM EST

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