Starred by 4 users

Owner:	dmblack@google.com
CC:	tbarzic@chromium.org dhadd...@chromium.org dmblack@google.com ckincaid@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Shell>HoldingSpace
Modified:	Nov 7, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
Hotlist-Merge-Approved
allpublic
reward-inprocess
reward-15000
Via-Wizard-Security
CVE_description-submitted
M-93
M-92
Target-92
external_security_report
FoundIn-92
LTS-Security-90
LTS-Security-NotApplicable-90
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
Release-1-M92
CVE-2021-30597

Issue 1232617: use after free in IsIndeterminate (chromeos version)

Reported by wxhu...@gmail.com on Sat, Jul 24, 2021, 1:54 AM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.107 Safari/537.36

Steps to reproduce the problem:
1.download a file, and pin a file
2.then remove it
3.browser crash

What is the expected behavior?

What went wrong?

```
==================================================================
==30544==ERROR: AddressSanitizer: heap-use-after-free on address 0x6130001334f8 at pc 0x55d4a3c5d7f5 bp 0x7ffe0d5b3d30 sp 0x7ffe0d5b3d28
READ of size 1 at 0x6130001334f8 thread T0 (chrome)
2021-07-24T05:51:37.574728Z ERROR chrome[30544:30663]: [object_proxy.cc(642)] Failed to call method: org.chromium.debugd.GetPerfOutputFd: object_path=
/org/chromium/debugd: org.freedesktop.DBus.Error.ServiceUnknown: The name org.chromium.debugd was not provided by any .service files
    #0 0x55d4a3c5d7f4 in has_value third_party/abseil-cpp/absl/types/optional.h:458:60
    #1 0x55d4a3c5d7f4 in IsIndeterminate ash/public/cpp/holding_space/holding_space_progress.cc:89:26
    #2 0x55d4a3c5d7f4 in ash::HoldingSpaceProgress::IsComplete() const ash/public/cpp/holding_space/holding_space_progress.cc:85:11
    #3 0x55d4a3c9a819 in ash::HoldingSpaceItemChipView::UpdateSecondaryAction() ash/system/holding_space/holding_space_item_chip_view.cc:468:57
    #4 0x55d49bf064d1 in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*) ui/events/event_dispatcher.cc:191:12
    #5 0x55d49bf05869 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #6 0x55d49bf052ab in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #7 0x55d49bf04fa2 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #8 0x55d4a0f4e6ac in views::internal::RootView::NotifyEnterExitOfDescendant(ui::MouseEvent const&, ui::EventType, views::View*, views::View*)
ui/views/widget/root_view.cc:774:49
    #9 0x55d4a0f4debb in views::internal::RootView::OnMouseMoved(ui::MouseEvent const&) ui/views/widget/root_view.cc:539:30
    #10 0x55d4a0f694a5 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc
    #11 0x55d49bf064d1 in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*) ui/events/event_dispatcher.cc:191:12
    #12 0x55d49bf05869 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #13 0x55d49bf052ab in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #14 0x55d49bf04fa2 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #15 0x55d49f232d90 in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #16 0x55d49f2293ca in aura::WindowEventDispatcher::SynthesizeMouseMoveEvent() ui/aura/window_event_dispatcher.cc:871:10
    #17 0x55d49854ced6 in Run base/callback.h:98:12
    #18 0x55d49854ced6 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:178:33
    #19 0x55d498592b71 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:360:23
    #20 0x55d4985920fa in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:260:36
    #21 0x55d4985936ec in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
    #22 0x55d49871e5fe in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_libevent.cc:207:55
    #23 0x55d498593f5c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:467:12
```

```
    #24 0x55d4984ae5f7 in base::RunLoop::Run(base::Location const&) base/run_loop.cc:134:14
    #25 0x55d48de820ea in content::BrowserMainLoop::RunMainMessageLoop() content/browser/browser_main_loop.cc:996:18
    #26 0x55d48de8762a in content::BrowserMainRunnerImpl::Run() content/browser/browser_main_runner_impl.cc:152:15
    #27 0x55d48de7b3e9 in content::BrowserMain(content::MainFunctionParams const&) content/browser/browser_main.cc:47:28
    #28 0x55d4981f9951 in content::RunBrowserProcessMain(content::MainFunctionParams const&, content::ContentMainDelegate*)
content/app/content_main_runner_impl.cc:595:10
    #29 0x55d4981fc69e in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:1084:10
    #30 0x55d4981fb915 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:953:12
    #31 0x55d4981f5bf6 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content/app/content_main.cc:386:36
    #32 0x55d4981f611b in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:412:10
    #33 0x55d489081f79 in ChromeMain chrome/app/chrome_main.cc:151:12
    #34 0x7fe6537a3bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310

0x6130001334f8 is located 248 bytes inside of 344-byte region [0x613000133400,0x613000133558)
freed by thread T0 (chrome) here:
    #0 0x55d48907fc9d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:152:3
    #1 0x55d4a3c5a654 in ~unique_ptr buildtools/third_party/libc++/trunk/include/memory:1550:19
    #2 0x55d4a3c5a654 in destroy buildtools/third_party/libc++/trunk/include/memory:829:15
    #3 0x55d4a3c5a654 in destroy<std::unique_ptr<ash::HoldingSpaceItem>, void> buildtools/third_party/libc++/trunk/include/__memory/allocator_traits.h:307:13
    #4 0x55d4a3c5a654 in __destruct_at_end buildtools/third_party/libc++/trunk/include/vector:428:9
    #5 0x55d4a3c5a654 in clear buildtools/third_party/libc++/trunk/include/vector:371:29
    #6 0x55d4a3c5a654 in std::__1::__vector_base<std::__1::unique_ptr<ash::HoldingSpaceItem, std::__1::default_delete<ash::HoldingSpaceItem> >,
std::__1::allocator<std::__1::unique_ptr<ash::HoldingSpaceItem, std::__1::default_delete<ash::HoldingSpaceItem> > > >::~__vector_base()
buildtools/third_party/libc++/trunk/include/vector:465:9
    #7 0x55d4a3c579ab in ~vector buildtools/third_party/libc++/trunk/include/vector:557:5
    #8 0x55d4a3c579ab in ash::HoldingSpaceModel::RemoveIf(base::RepeatingCallback<bool (ash::HoldingSpaceItem const*)>)
ash/public/cpp/holding_space/holding_space_model.cc:193:1
    #9 0x55d4a3c7155b in ash::HoldingSpaceViewDelegate::ExecuteCommand(int, int) ash/system/holding_space/holding_space_view_delegate.cc:502:47
    #10 0x55d4a0dec2a6 in views::MenuModelAdapter::ExecuteCommand(int, int) ui/views/controls/menu/menu_model_adapter.cc:169:12
    #11 0x55d4a0e264e9 in views::internal::MenuRunnerImpl::OnMenuClosed(views::internal::MenuControllerDelegate::NotifyType, views::MenuItemView*, int)
ui/views/controls/menu/menu_runner_impl.cc:245:29
    #12 0x55d4a0e02a88 in views::MenuController::ExitMenu() ui/views/controls/menu/menu_controller.cc:3139:13
    #13 0x55d4a0e077f6 in views::MenuController::OnMouseReleased(views::SubmenuView*, ui::MouseEvent const&) ui/views/controls/menu/menu_controller.cc:827:7
    #14 0x55d4a0f69322 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc:1463:20
    #15 0x55d49bf064d1 in ui::EventDispatcher::DispatchEvent(ui::EventHandler*, ui::Event*) ui/events/event_dispatcher.cc:191:12
    #16 0x55d49bf05869 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #17 0x55d49bf052ab in ui::EventDispatcherDelegate::DispatchEventToTarget(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:84:14
    #18 0x55d49bf04fa2 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #19 0x55d49f232d90 in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #20 0x55d49bf0a516 in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:113:16
    #21 0x55d49bf0aabe in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*) ui/events/event_source.cc:60:14
    #22 0x55d4909c9738 in ui::EventRewriterChromeOS::RewriteMouseButtonEvent(ui::MouseEvent const&, base::WeakPtr<ui::EventRewriterContinuation>)
ui/chromeos/events/event_rewriter_chromeos.cc:1259:12
    #23 0x55d4909c9bd7 in ui::EventRewriterChromeOS::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>)
ui/chromeos/events/event_rewriter_chromeos.cc:769:12
    #24 0x55d49bf0aa52 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*) ui/events/event_source.cc:61:32
    #25 0x55d4a375b6ff in ash::KeyboardDrivenEventRewriter::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>)
ash/events/keyboard_driven_event_rewriter.cc:31:12
    #26 0x55d49bf0aa52 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*) ui/events/event_source.cc:61:32
    #27 0x55d4a37568a2 in ash::AccessibilityEventRewriter::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>) base/memory/weak_ptr.h
    #28 0x55d49bf0aa52 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*) ui/events/event_source.cc:61:32
    #29 0x55d4a3571947 in ash::AutoclickDragEventRewriter::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>)
ash/accessibility/autoclick/autoclick_drag_event_rewriter.cc
    #30 0x55d49bf0aa52 in ui::EventSource::EventRewriterContinuationImpl::SendEvent(ui::Event const*) ui/events/event_source.cc:61:32
    #31 0x55d4a354d8b2 in ash::FullscreenMagnifierController::RewriteEvent(ui::Event const&, base::WeakPtr<ui::EventRewriterContinuation>)
ash/accessibility/magnifier/fullscreen_magnifier_controller.cc
    #32 0x55d49bf0a148 in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*) ui/events/event_source.cc:139:29
    #33 0x55d4a37966ca in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*) ui/aura/window_tree_host_platform.cc:247:38
    #34 0x55d4a379f3ae in ash::AshWindowTreeHostPlatform::DispatchEvent(ui::Event*) ash/host/ash_window_tree_host_platform.cc:184:40
    #35 0x55d49bf157b4 in Run base/callback.h:98:12
    #36 0x55d49bf157b4 in ui::DispatchEventFromNativeUiEvent(ui::Event* const&, base::OnceCallback<void (ui::Event*)>) ui/events/ozone/events_ozone.cc:36:25

previously allocated by thread T0 (chrome) here:
    #0 0x55d48907f43d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:95:3
    #1 0x55d4a3c5bc68 in ash::HoldingSpaceItem::Deserialize(base::DictionaryValue const&, base::OnceCallback<std::__1::unique_ptr<ash::HoldingSpaceImage,
std::__1::default_delete<ash::HoldingSpaceImage> > (ash::HoldingSpaceItem::Type, base::FilePath const&)>) ash/public/cpp/holding_space/holding_space_item.cc:102:27
    #2 0x55d4a5a8012d in ash::HoldingSpacePersistenceDelegate::RestoreModelFromPersistence()
chrome/browser/ui/ash/holding_space/holding_space_persistence_delegate.cc:147:9
    #3 0x55d4a5a6617a in ash::HoldingSpaceKeyedService::InitializeDelegates() chrome/browser/ui/ash/holding_space/holding_space_keyed_service.cc:406:15
    #4 0x55d4a5a620b4 in ash::HoldingSpaceKeyedService::OnProfileReady() chrome/browser/ui/ash/holding_space/holding_space_keyed_service.cc:352:3
    #5 0x55d4a5a7f7b3 in ash::HoldingSpaceKeyedServiceFactory::BuildServiceInstanceFor(content::BrowserContext*) const
chrome/browser/ui/ash/holding_space/holding_space_keyed_service_factory.cc:71:14
    #6 0x55d49e0307a5 in KeyedServiceFactory::GetServiceForContext(void*, bool) components/keyed_service/core/keyed_service_factory.cc:80:15
    #7 0x55d4a5a7f564 in ash::HoldingSpaceKeyedServiceFactory::GetService(content::BrowserContext*)
chrome/browser/ui/ash/holding_space/holding_space_keyed_service_factory.cc:42:22
    #8 0x55d491ea389a in ash::UserSessionInitializer::OnUserSessionStarted(bool) chrome/browser/ash/login/session/user_session_initializer.cc:243:51
    #9 0x55d4a22a28f5 in session_manager::SessionManager::SessionStarted() components/session_manager/core/session_manager.cc:74:14
    #10 0x55d491ea23aa in ash::ChromeSessionManager::SessionStarted() chrome/browser/ash/login/session/chrome_session_manager.cc:252:36
    #11 0x55d491ea1f94 in ash::(anonymous namespace)::StartUserSession(Profile*, std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> >
const&) chrome/browser/ash/login/session/chrome_session_manager.cc:160:45
    #12 0x55d491ea15f8 in ash::ChromeSessionManager::Initialize(base::CommandLine const&, Profile*, bool)
chrome/browser/ash/login/session/chrome_session_manager.cc:248:3
    #13 0x55d4922f0e49 in chromeos::ChromeBrowserMainPartsChromeos::PostProfileInit() chrome/browser/chromeos/chrome_browser_main_chromeos.cc:1044:58
    #14 0x55d49905cad7 in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome/browser/chrome_browser_main.cc:1466:3
    #15 0x55d49905b303 in ChromeBrowserMainParts::PreMainMessageLoopRun() chrome/browser/chrome_browser_main.cc:1054:18
    #16 0x55d4922ed7c1 in chromeos::ChromeBrowserMainPartsChromeos::PreMainMessageLoopRun()
chrome/browser/chromeos/chrome_browser_main_chromeos.cc:713:39
    #17 0x55d48de800b7 in content::BrowserMainLoop::PreMainMessageLoopRun() content/browser/browser_main_loop.cc:946:28
    #18 0x55d48ee8f92f in Run base/callback.h:98:12
    #19 0x55d48ee8f92f in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:41:29
    #20 0x55d48de7f5ee in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:854:25
    #21 0x55d48de86c3d in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) content/browser/browser_main_runner_impl.cc:131:15
    #22 0x55d48de7b389 in content::BrowserMain(content::MainFunctionParams const&) content/browser/browser_main.cc:43:32
    #23 0x55d4981f9951 in content::RunBrowserProcessMain(content::MainFunctionParams const&, content::ContentMainDelegate*)
content/app/content_main_runner_impl.cc:595:10
    #24 0x55d4981fc69e in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:1084:10
    #25 0x55d4981fb915 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:953:12
    #26 0x55d4981f5bf6 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content/app/content_main.cc:386:36
    #27 0x55d4981f611b in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:412:10
    #28 0x55d489081f79 in ChromeMain chrome/app/chrome_main.cc:151:12
    #29 0x7fe6537a3bf6 in __libc_start_main /build/glibc-S9d2JN/glibc-2.27/csu/../csu/libc-start.c:310

SUMMARY: AddressSanitizer: heap-use-after-free third_party/abseil-cpp/absl/types/optional.h:458:60 in has_value
```

```
Shadow bytes around the buggy address:
  0x0c268001e640: fa fa fa fa fa fa fa fa 00 00 00 00 00 00 00 00
  0x0c268001e650: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c268001e660: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0c268001e670: 00 00 00 00 fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c268001e680: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c268001e690: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd[fd]
  0x0c268001e6a0: fd fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa
  0x0c268001e6b0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c268001e6c0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c268001e6d0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c268001e6e0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa 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
==30544==ABORTING
```

Did this work before? N/A

Chrome version: 92.0.4515.107 Channel: stable
OS Version: 10.0

Comment 1 by sheriffbot on Sat, Jul 24, 2021, 1:57 AM EDT Project Member

Labels: external_security_report

Comment 2 by wxhu...@gmail.com on Sat, Jul 24, 2021, 1:58 AM EDT

my chormium version is 93.0.4564.0

poc.mp4
8.8 MB View Download

Comment 3 by dominickn@chromium.org on Sat, Jul 24, 2021, 2:16 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: dmblack@google.com
Cc: tbarzic@chromium.org
Labels: -OS-Windows Security_Severity-Medium FoundIn-92 OS-Chrome
Components: UI>Shell>HoldingSpace

+holding space folks, can you take a look? Assigning medium severity as this isn't web accessible, but is still a browser process UaF.

Comment 4 by sheriffbot on Sat, Jul 24, 2021, 2:21 AM EDT Project Member

Labels: Security_Impact-Stable

Comment 5 by sheriffbot on Sat, Jul 24, 2021, 9:06 AM EDT Project Member

Labels: M-92 Target-92

Setting milestone and target because of medium severity.

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

Comment 6 by sheriffbot on Sat, Jul 24, 2021, 9:07 AM EDT Project Member

Labels: -Pri-2 Pri-1

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

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

Comment 7 by dmblack@google.com on Sat, Jul 24, 2021, 3:05 PM EDT Project Member

Fix out for review: https://chromium-review.googlesource.com/c/chromium/src/+/3050659

Comment 8 by dmblack@google.com on Sat, Jul 24, 2021, 3:06 PM EDT Project Member

Status: Started (was: Assigned)

Comment 9 by Git Watcher on Sat, Jul 24, 2021, 5:54 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/78c7594b44c23a53a640331967df526865234ef7

commit 78c7594b44c23a53a640331967df526865234ef7
Author: David Black <dmblack@google.com>
Date: Sat Jul 24 21:53:55 2021

Fix potential UAF in holding space item views.

Holding space items in the model can be destroyed before their
associated views. When this happens, its possible that the view will
still receive a mouse exited event if it had been hovered over.

When hover state changes, the holding space item view attempts to look
at the underlying item to update UI state. But by that time, the item
has already been deleted.

~~Bug: 1232617~~
Change-Id: I6aa4169518fa8e17abd2194d009780fcc6d12d3a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3050659
Reviewed-by: Toni Barzić <tbarzic@chromium.org>
Commit-Queue: David Black <dmblack@google.com>
Cr-Commit-Position: refs/heads/master@{#905067}

[modify] https://crrev.com/78c7594b44c23a53a640331967df526865234ef7/ash/system/holding_space/holding_space_item_chip_view.cc
[modify] https://crrev.com/78c7594b44c23a53a640331967df526865234ef7/ash/system/holding_space/holding_space_item_screen_capture_view.cc
[modify] https://crrev.com/78c7594b44c23a53a640331967df526865234ef7/ash/system/holding_space/holding_space_item_view.cc
[modify] https://crrev.com/78c7594b44c23a53a640331967df526865234ef7/ash/system/holding_space/holding_space_item_view.h

Comment 10 by dmblack@google.com on Sat, Jul 24, 2021, 6:28 PM EDT Project Member

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

Requesting merge request to M-93 and (if possible) M-92. Fixes a UAF.

Comment 11 by sheriffbot on Sat, Jul 24, 2021, 6:34 PM EDT Project Member

Labels: -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: Request affecting a post-stable build
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), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 12 by dmblack@google.com on Sat, Jul 24, 2021, 7:36 PM EDT Project Member

Cc: dhadd...@chromium.org

1. Yes
2. https://chromium-review.googlesource.com/c/chromium/src/+/3050659
3. Yes
4. M-93 and, if possible, M-92
5. UAF discovered post branch
6. No
7. No
8. +dhaddock@

Comment 13 by sheriffbot on Sun, Jul 25, 2021, 6:31 PM EDT Project Member

Labels: -Merge-Request-93 Hotlist-Merge-Approved Merge-Approved-93

Your change meets the bar and is auto-approved for M93. Please go ahead and merge the CL to branch 4577 (refs/branch-heads/4577) manually. Please contact milestone owner if you have questions.
Merge instructions: https://www.chromium.org/developers/how-tos/drover
Owners: benmason@(Android), govind@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 14 by Git Watcher on Sun, Jul 25, 2021, 11:39 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/97a7169f23db55418d1d7a062792ead237343d70

commit 97a7169f23db55418d1d7a062792ead237343d70
Author: David Black <dmblack@google.com>
Date: Mon Jul 26 03:38:23 2021

Fix potential UAF in holding space item views.

Holding space items in the model can be destroyed before their
associated views. When this happens, its possible that the view will
still receive a mouse exited event if it had been hovered over.

When hover state changes, the holding space item view attempts to look
at the underlying item to update UI state. But by that time, the item
has already been deleted.

(cherry picked from commit 78c7594b44c23a53a640331967df526865234ef7)

~~Bug: 1232617~~
Change-Id: I6aa4169518fa8e17abd2194d009780fcc6d12d3a

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3050659
Reviewed-by: Toni Baržić <tbarzic@chromium.org>
Commit-Queue: David Black <dmblack@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#905067}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3053270
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4577@{#138}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/97a7169f23db55418d1d7a062792ead237343d70/ash/system/holding_space/holding_space_item_chip_view.cc
[modify] https://crrev.com/97a7169f23db55418d1d7a062792ead237343d70/ash/system/holding_space/holding_space_item_screen_capture_view.cc
[modify] https://crrev.com/97a7169f23db55418d1d7a062792ead237343d70/ash/system/holding_space/holding_space_item_view.cc
[modify] https://crrev.com/97a7169f23db55418d1d7a062792ead237343d70/ash/system/holding_space/holding_space_item_view.h

Comment 15 by dmblack@google.com on Mon, Jul 26, 2021, 3:38 PM EDT Project Member

~~Issue 1207994~~ has been merged into this issue.

Comment 16 by dgagnon@google.com on Wed, Jul 28, 2021, 8:39 PM EDT Project Member

Labels: -Hotlist-Merge-Review -Merge-Review-92 Merge-Approved-92

If this is considered a safe change, merge approved for M92

Comment 17 by Git Watcher on Fri, Jul 30, 2021, 1:35 PM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/514c0377a6a1ff3c505b8ea0f3919d60f488e041

commit 514c0377a6a1ff3c505b8ea0f3919d60f488e041
Author: David Black <dmblack@google.com>
Date: Fri Jul 30 17:34:36 2021

[M92] Fix potential UAF in holding space item views.

Holding space items in the model can be destroyed before their
associated views. When this happens, its possible that the view will
still receive a mouse exited event if it had been hovered over.

When hover state changes, the holding space item view attempts to look
at the underlying item to update UI state. But by that time, the item
has already been deleted.

(cherry picked from commit 78c7594b44c23a53a640331967df526865234ef7)

~~Bug: 1232617~~
Change-Id: I6aa4169518fa8e17abd2194d009780fcc6d12d3a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3050659
Reviewed-by: Toni Baržić <tbarzic@chromium.org>
Commit-Queue: David Black <dmblack@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#905067}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3062630
Cr-Commit-Position: refs/branch-heads/4515@{#1931}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/514c0377a6a1ff3c505b8ea0f3919d60f488e041/ash/system/holding_space/holding_space_item_chip_view.cc
[modify] https://crrev.com/514c0377a6a1ff3c505b8ea0f3919d60f488e041/ash/system/holding_space/holding_space_item_screen_capture_view.cc
[modify] https://crrev.com/514c0377a6a1ff3c505b8ea0f3919d60f488e041/ash/system/holding_space/holding_space_item_view.cc
[modify] https://crrev.com/514c0377a6a1ff3c505b8ea0f3919d60f488e041/ash/system/holding_space/holding_space_item_view.h

Comment 18 by dmblack@google.com on Fri, Jul 30, 2021, 1:43 PM EDT Project Member

Status: Fixed (was: Started)

Comment 19 by sheriffbot on Sat, Jul 31, 2021, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Sat, Jul 31, 2021, 1:40 PM EDT Project Member

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

Comment 21 by amyressler@chromium.org on Mon, Aug 2, 2021, 10:29 AM EDT Project Member

Labels: Release-1-M92

Comment 22 by amyressler@google.com on Mon, Aug 2, 2021, 10:57 AM EDT Project Member

Labels: CVE-2021-30597 CVE_description-missing

Comment 23 by amyressler@google.com on Wed, Aug 11, 2021, 2:25 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 24 by amyressler@chromium.org on Wed, Aug 11, 2021, 3:11 PM EDT Project Member

Congratulations, the VRP Panel has decided to award you $15,000 for this report. Nice work!

Comment 25 by wxhu...@gmail.com on Wed, Aug 11, 2021, 6:35 PM EDT

Thanks a lot.

Comment 26 by amyressler@google.com on Fri, Aug 13, 2021, 11:41 AM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 27 by amyressler@google.com on Thu, Aug 26, 2021, 1:09 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 28 by voit@google.com on Mon, Sep 6, 2021, 6:16 AM EDT Project Member

Labels: LTS-Security-90 LTS-Security-NotApplicable-90

Not reproducible on M90, so no need to merge the fix to LTS.

Comment 29 by sheriffbot on Sun, Nov 7, 2021, 1:29 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