☆ Starred by 3 users

Owner:	updowndota@google.com
CC:	rzanoni@google.com xiy...@chromium.org ceb@google.com xiaoh...@chromium.org ellyj...@chromium.org dgagnon@google.com
Status:	Fixed *(Closed)*
Components:	UI
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-3000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
M-98
Merge-Approved-100
Target-98
FoundIn-96
Security_Impact-Extended
merge-merged-4664
Merge-Merged-96
LTS-Merge-Merged-96
Merge-Review-98
merge-merged-4844
merge-merged-99
Release-1-M99
CVE-2022-0977

Issue 1299225: Security: Heap-use-after-free in QuickAnswersUiController::CloseQuickAnswersView

Reported by chrom...@gmail.com on Sat, Feb 19, 2022, 6:06 PM EST

Code

Chrome Version: 101.0.4897.0
Operating System: chromeOS Ozone x11

REPRODUCTION CASE

1. Open the testcase and click on the button
2. Select any text on the popup page then right-click and wait
4. On the testcase page Right-click

```
==19538==ERROR: AddressSanitizer: heap-use-after-free on address 0x6180003f1880 at pc 0x559e234dad5c bp
0x7ffeefbbc0f0 sp 0x7ffeefbbc0e8
READ of size 8 at 0x6180003f1880 thread T0 (chrome)
==19538==WARNING: invalid path to external symbolizer!
==19538==WARNING: Failed to use and restart external symbolizer!
    #0 0x559e234dad5b in QuickAnswersUiController::CloseQuickAnswersView()
./../../chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc:73:26
    #1 0x559e234d9134 in QuickAnswersControllerImpl::DismissQuickAnswers(quick_answers::QuickAnswersExitPoint)
./../../chrome/browser/ui/quick_answers/quick_answers_controller_impl.cc:138:47
    #2 0x559e35bb4ac1 in RenderViewContextMenuBase::MenuClosed(ui::SimpleMenuModel*)
./../../components/renderer_context_menu/render_view_context_menu_base.cc:435:14
    #3 0x559e282b4066 in Run ./../../base/callback.h:142:12
    #4 0x559e282b4066 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
    #5 0x559e282f5cb7 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:29)>
./../../base/task/common/task_annotator.h:74:5
    #6 0x559e282f5cb7 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:385:21
    #7 0x559e282f53b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:290:41
    #8 0x559e282f6951 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #9 0x559e2843791d in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_libevent.cc:195:55
    #10 0x559e282f700a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
    #11 0x559e2822e0dc in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:141:14
    #12 0x559e1ed12062 in content::BrowserMainLoop::RunMainMessageLoop()
./../../content/browser/browser_main_loop.cc:1056:18
    #13 0x559e1ed165e1 in content::BrowserMainRunnerImpl::Run()
./../../content/browser/browser_main_runner_impl.cc:155:15
    #14 0x559e1ed0c40a in content::BrowserMain(content::MainFunctionParams)

./../../content/browser/browser_main.cc:30:28
    #15 0x559e2800bf7f in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*)
./../../content/app/content_main_runner_impl.cc:642:10
```

```
./../../content/app/content_main_runner_impl.cc:642:10
    #16 0x559e2800eac8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./../../content/app/content_main_runner_impl.cc:1175:10
    #17 0x559e2800df18 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1042:12
    #18 0x559e280086f9 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:401:36
    #19 0x559e28008d75 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:429:10
    #20 0x559e1a0db5ea in ChromeMain ./../../chrome/app/chrome_main.cc:176:12
    #21 0x7fc4313f10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

0x6180003f1880 is located 0 bytes inside of 840-byte region [0x6180003f1880,0x6180003f1bc8)
freed by thread T0 (chrome) here:
    #0 0x559e1a0d962d 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 0x559e2e0a5e05 in operator() ./../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:54:5
    #2 0x559e2e0a5e05 in reset ./../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:315:7
    #3 0x559e2e0a5e05 in ~unique_ptr ./../../buildtools/third_party/libc++/trunk/include/__memory/unique_ptr.h:269:19
    #4 0x559e2e0a5e05 in views::View::DoRemoveChildView(views::View*, bool, bool, views::View*)
./../../ui/views/view.cc:2638:1
    #5 0x559e2e0a6037 in views::View::RemoveAllChildViews() ./../../ui/views/view.cc:328:5
    #6 0x559e2e0dc950 in views::Widget::DestroyRootView() ./../../ui/views/widget/widget.cc:1779:15
    #7 0x559e2e0dc5f0 in views::Widget::~Widget() ./../../ui/views/widget/widget.cc:206:3
    #8 0x559e2e0dcb61 in views::Widget::~Widget() ./../../ui/views/widget/widget.cc:187:19
    #9 0x559e2e12ebba in views::NativeWidgetAura::~NativeWidgetAura() ./../../ui/views/widget/native_widget_aura.cc:0:0
    #10 0x559e2e12ee37 in views::NativeWidgetAura::~NativeWidgetAura()
./../../ui/views/widget/native_widget_aura.cc:1132:39
    #11 0x559e2dc8d247 in aura::Window::~Window() ./../../ui/aura/window.cc:227:16
    #12 0x559e2dc8e453 in aura::Window::~Window() ./../../ui/aura/window.cc:182:19
    #13 0x559e2dc8e00d in aura::Window::RemoveOrDestroyChildren() ./../../ui/aura/window.cc:937:7
    #14 0x559e2dc8d1ca in aura::Window::~Window() ./../../ui/aura/window.cc:219:3
    #15 0x559e2dc8e453 in aura::Window::~Window() ./../../ui/aura/window.cc:182:19
    #16 0x559e282b4066 in Run ./../../base/callback.h:142:12
    #17 0x559e282b4066 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
    #18 0x559e282f5cb7 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:29)>
./../../base/task/common/task_annotator.h:74:5
    #19 0x559e282f5cb7 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:385:21
    #20 0x559e282f53b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:290:41
    #21 0x559e282f6951 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #22 0x559e2843791d in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_libevent.cc:195:55
    #23 0x559e282f700a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
    #24 0x559e2822e0dc in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:141:14
    #25 0x559e1ed12062 in content::BrowserMainLoop::RunMainMessageLoop()

./../../content/browser/browser_main_loop.cc:1056:18
    #26 0x559e1ed165e1 in content::BrowserMainRunnerImpl::Run()
./../../content/browser/browser_main_runner_impl.cc:155:15
```

```
./../../content/browser/browser_main_runner_impl.cc:155:15
   #27 0x559e1ed0c40a in content::BrowserMain(content::MainFunctionParams)
./../../content/browser/browser_main.cc:30:28
   #28 0x559e2800bf7f in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*)
./../../content/app/content_main_runner_impl.cc:642:10
   #29 0x559e2800eac8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./../../content/app/content_main_runner_impl.cc:1175:10
   #30 0x559e2800df18 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1042:12
   #31 0x559e280086f9 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:401:36
   #32 0x559e28008d75 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:429:10
   #33 0x559e1a0db5ea in ChromeMain ./../../chrome/app/chrome_main.cc:176:12
   #34 0x7fc4313f10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

previously allocated by thread T0 (chrome) here:
   #0 0x559e1a0d8dcd 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 0x559e234dabd0 in QuickAnswersUiController::CreateQuickAnswersView(gfx::Rect const&,
std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&, std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, bool)
./../../chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc:56:25
   #2 0x559e234d8d0a in QuickAnswersControllerImpl::HandleQuickAnswerRequest(quick_answers::QuickAnswersRequest
const&) ./../../chrome/browser/ui/quick_answers/quick_answers_controller_impl.cc:123:35
   #3 0x559e234d89b9 in QuickAnswersControllerImpl::MaybeShowQuickAnswers(gfx::Rect const&,
std::__1::basic_string<char, std::__1::char_traits<char>, std::__1::allocator<char> > const&, quick_answers::Context const&)
./../../chrome/browser/ui/quick_answers/quick_answers_controller_impl.cc:110:5
   #4 0x559e3550cdcd in QuickAnswersMenuObserver::OnTextSurroundingSelectionAvailable(std::__1::basic_string<char,
std::__1::char_traits<char>, std::__1::allocator<char> > const&, std::__1::basic_string<char16_t,
std::__1::char_traits<char16_t>, std::__1::allocator<char16_t> > const&, unsigned int, unsigned int)
./../../chrome/browser/renderer_context_menu/quick_answers_menu_observer.cc:142:34
   #5 0x559e1d307d1c in Run ./../../base/callback.h:142:12
   #6 0x559e1d307d1c in
blink::mojom::LocalFrame_GetTextSurroundingSelection_ForwardToCallback::Accept(mojo::Message*)
./gen/third_party/blink/public/mojom/frame/frame.mojom.cc:9500:26
   #7 0x559e29a842c7 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
./../../mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:896:23
   #8 0x559e29a96bd7 in mojo::MessageDispatcher::Accept(mojo::Message*)
./../../mojo/public/cpp/bindings/lib/message_dispatcher.cc:43:19
   #9 0x559e29a86f56 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)
./../../mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:658:20
   #10 0x559e29a494e9 in IPC::(anonymous
namespace)::ChannelAssociatedGroupController::AcceptOnEndpointThread(mojo::Message)
./../../ipc/ipc_mojo_bootstrap.cc:1008:24
   #11 0x559e29a4315b in Invoke<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>
./../../base/bind_internal.h:542:12
   #12 0x559e29a4315b in MakeItSo<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>, mojo::Message>
./../../base/bind_internal.h:706:12
   #13 0x559e29a4315b in RunImpl<void (IPC::(anonymous namespace)::ChannelAssociatedGroupController::*)
(mojo::Message), std::__1::tuple<scoped_refptr<IPC::(anonymous namespace)::ChannelAssociatedGroupController>,

mojo::Message>, 0UL, 1UL> ./../../base/bind_internal.h:779:12
   #14 0x559e29a4315b in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous
namespace)::ChannelAssociatedGroupController::*)(mojo::Message), scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController::*)(mojo::Message), scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController>, mojo::Message>, void ()>::RunOnce(base::internal::BindStateBase*)
./../../base/bind_internal.h:748:12
    #15 0x559e282b4066 in Run ./../../base/callback.h:142:12
    #16 0x559e282b4066 in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)
./../../base/task/common/task_annotator.cc:135:32
    #17 0x559e282f5cb7 in RunTask<(lambda at
../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:387:29)>
./../../base/task/common/task_annotator.h:74:5
    #18 0x559e282f5cb7 in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:385:21
    #19 0x559e282f53b7 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:290:41
    #20 0x559e282f6951 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:0:0
    #21 0x559e2843791d in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*)
./../../base/message_loop/message_pump_libevent.cc:195:55
    #22 0x559e282f700a in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta) ./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:497:12
    #23 0x559e2822e0dc in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:141:14
    #24 0x559e1ed12062 in content::BrowserMainLoop::RunMainMessageLoop()
./../../content/browser/browser_main_loop.cc:1056:18
    #25 0x559e1ed165e1 in content::BrowserMainRunnerImpl::Run()
./../../content/browser/browser_main_runner_impl.cc:155:15
    #26 0x559e1ed0c40a in content::BrowserMain(content::MainFunctionParams)
./../../content/browser/browser_main.cc:30:28
    #27 0x559e2800bf7f in content::RunBrowserProcessMain(content::MainFunctionParams, content::ContentMainDelegate*)
./../../content/app/content_main_runner_impl.cc:642:10
    #28 0x559e2800eac8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)
./../../content/app/content_main_runner_impl.cc:1175:10
    #29 0x559e2800df18 in content::ContentMainRunnerImpl::Run() ./../../content/app/content_main_runner_impl.cc:1042:12
    #30 0x559e280086f9 in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)
./../../content/app/content_main.cc:401:36
    #31 0x559e28008d75 in content::ContentMain(content::ContentMainParams) ./../../content/app/content_main.cc:429:10
    #32 0x559e1a0db5ea in ChromeMain ./../../chrome/app/chrome_main.cc:176:12
    #33 0x7fc4313f10b2 in __libc_start_main /build/glibc-eX1tMB/glibc-2.31/csu/../csu/libc-start.c:308:16

SUMMARY: AddressSanitizer: heap-use-after-free (/home/lbstyle/Desktop/asan-linux-release-973094/chrome+0x1720ed5b)
(BuildId: 0aca5d3f0a92ae2f)
Shadow bytes around the buggy address:
  0x0c30800762c0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c30800762d0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c30800762e0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c30800762f0: fd fd fd fd fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3080076300: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c3080076310:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3080076320: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3080076330: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3080076340: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd

  0x0c3080076350: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3080076360: 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):
```

```
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
==19538==ABORTING
```

[Deleted] **Screencast from 19 23:56:52 01+ 2022 ,فبراير.webm**

testcase.html
335 bytes View Download

Comment 1 by sheriffbot on Sat, Feb 19, 2022, 6:07 PM EST

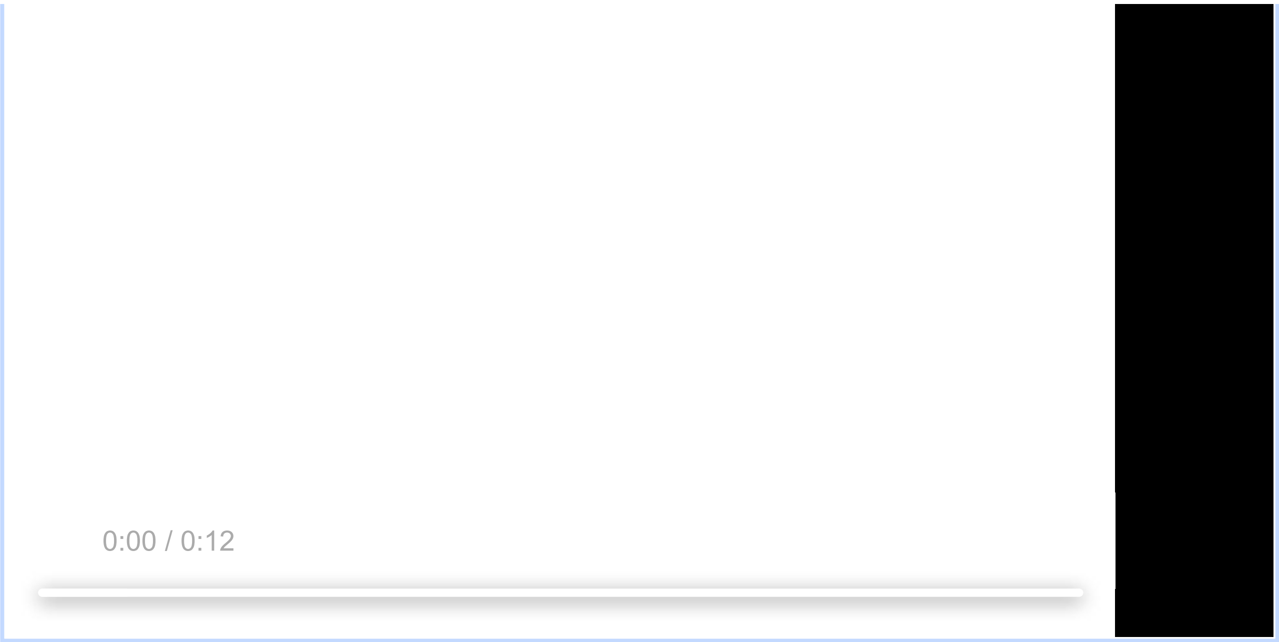
Labels: external_security_report

Comment 2 Deleted

Comment 3 by chrom...@gmail.com on Sun, Feb 20, 2022, 12:20 AM EST

Screencast from 20 06:19:41 01+ 2022 ,فبراير.webm
2.0 MB View Download

[redacted]



Comment 4 by danakj@chromium.org on Tue, Feb 22, 2022, 5:02 PM EST

Status: Assigned (was: Unconfirmed)
Owner: updowndota@google.com
Cc: ellyj...@chromium.org xiy...@chromium.org xiaoh...@chromium.org
Labels: Security_Severity-Critical FoundIn-96 Pri-2
Components: UI

QuickAnswersUiController has a pointer to a View which is owned by the hierarchy, as the comment says.

But then it uses that pointer without somehow observing if the pointer is deleted, causing a UAF. This requires pretty reasonable user interaction so not decreasing the impact. The pointer in question has been present for a year now, so on all released browsers.

Interestingly, this would potentially be mitigated by raw_ptr, if it ships, but this was missed in the raw_ptr rewrite: https://bugs.chromium.org/p/chromium/issues/detail?id=1299932

I can not repro on Linux, as the given UI element does not pop up. So I will have to ask the related team to have a look. If this is not in M96 please update.

Comment 5 by danakj@chromium.org on Tue, Feb 22, 2022, 5:02 PM EST

Labels: OS-Chrome

Comment 6 by sheriffbot on Tue, Feb 22, 2022, 5:05 PM EST

Labels: Security_Impact-Extended

Comment 7 by ellyj...@chromium.org on Tue, Feb 22, 2022, 5:15 PM EST

This UAF happens because the code assumes that QuickAnswersMenuObserver::OnMenuClosed() can only happen before the QuickAnswersView itself is destroyed, but there is no guarantee of this in the presence of async window closure, and the code (as danakj@ said in #4) makes incorrect assumptions about the lifetime of the View, which it does not own.

In general there are a couple of ways to deal with this:

1. ViewTracker instead of raw View* to hold the View (but this has a runtime cost)

1. ViewTracker instead of raw View* to hold the View (but this has a runtime cost)
2. Hold a WeakPtr to QuickAnswersView instead (it already supports WeakPtr)
3. Something else

QuickAnswersView is doing some unusual stuff like manually creating its own Widget as part of View construction which also makes the lifetime harder to reason about.

Comment 8 by xiy...@chromium.org on Tue, Feb 22, 2022, 5:26 PM EST

The video is very informative that the QuickAnswersView widget could be closed by closing the browser window. So the assumption that the widget has to be closed via QuickAnswersView does not stand.

One quick fix could be adding a

```
  void OnQuickAnswersViewDestroyed();
```

to QuickAnswersUiController and QuickAnswersView calls it from its dtor to reset the reference.

We have similar problem with `user_consent_view_` as well.

Comment 9 by sheriffbot on Thu, Feb 24, 2022, 12:47 PM EST

Labels: M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 10 by sheriffbot on Thu, Feb 24, 2022, 1:13 PM EST

Labels: -Pri-2 Pri-0

Setting Pri-0 to match security severity Critical. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 11 by betuls@google.com on Sun, Feb 27, 2022, 10:54 PM EST

Hi updowndota@,
What is the latest status on this bug?

Comment 12 by betuls@google.com on Mon, Feb 28, 2022, 1:27 PM EST

Labels: -Security_Severity-Critical Security_Severity-Medium

Maiking this P1 based on
https://chromium.googlesource.com/chromiumos/docs/+/refs/heads/main/security_severity_guidelines.md

Comment 13 by updowndota@google.com on Mon, Feb 28, 2022, 1:36 PM EST

Status: Started (was: Assigned)

Comment 14 by betuls@google.com on Mon, Feb 28, 2022, 3:49 PM EST

Labels: Pri-1

Comment 15 by danakj@chromium.org on Tue, Mar 1, 2022, 12:31 PM EST

Could you clarify why this is medium severity? That is generally for bugs that are very mitigated - such requiring complex user interaction.

Comment 16 by danakj@chromium.org on Tue, Mar 1, 2022, 12:33 PM EST

It looks like we have 2 competing ideas of severity:
https://chromium.googlesource.com/chromium/src/+/HEAD/docs/security/severity-guidelines.md#TOC-Low-severity

This one is in Chrome so I think the Chrome ones apply.

Comment 17 by danakj@chromium.org on Tue, Mar 1, 2022, 12:37 PM EST

Labels: -Security_Severity-Medium Security_Severity-High

This is at least high sev according to both: "A Chrome sandbox escapes allows bypassing the Chrome sandbox." and a browser UAF is a tool used to escape the sandbox. Idk how to reconcile critical between these two.

Comment 18 by chrom...@gmail.com on Tue, Mar 1, 2022, 12:48 PM EST

Sounds reasonable.

Since this is a UAF in the browser process, this would be a Critical, but the gesture/user-interaction lowers it to High.

Comment 19 by Git Watcher on Wed, Mar 2, 2022, 4:20 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c

commit 7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c
Author: Yue Li <updowndota@google.com>
Date: Wed Mar 02 09:19:15 2022

Quick Answers: Fix timing issue on view destruction

Call the UI controller on view destruction to avoid possible timing
issue.

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: Ice5a7a13324b3b68442bd91073f513c535f51c15
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499463
Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
Commit-Queue: Yue Li <updowndota@chromium.org>
Cr-Commit-Position: refs/heads/main@{#976595}

[modify]
https://crrev.com/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c/chrome/browser/ui/quick_answers/ui/user_consent_view.cc
[modify]
https://crrev.com/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c/chrome/browser/ui/quick_answers/ui/quick_answers_view.cc
[modify]
https://crrev.com/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify]

[modify]
https://crrev.com/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c/chrome/browser/ui/quick_answers/test/chrome_quick_answers_test_base.cc
[modify]
https://crrev.com/7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc

Comment 20 by updowndota@google.com on Wed, Mar 2, 2022, 4:35 AM EST

Status: Fixed (was: Started)

Comment 21 by Git Watcher on Wed, Mar 2, 2022, 10:58 AM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f9beeea17c09e39c8187caa67b938a1688829d0b

commit f9beeea17c09e39c8187caa67b938a1688829d0b
Author: Sergey Poromov <poromov@chromium.org>
Date: Wed Mar 02 15:57:31 2022

Revert "Quick Answers: Fix timing issue on view destruction"

This reverts commit 7c822d7f1e932fbc4a1220a6f1c5f69b88034f1c.

Reason for revert: Consistent failures on Chrome OS Asan/Lsan builder:
https://ci.chromium.org/p/chromium/builders/ci/Linux%20Chromium%20OS%20ASan%20LSan%20Tests%20%281%29

First failure:
https://ci.chromium.org/ui/p/chromium/builders/ci/Linux%20Chromium%20OS%20ASan%20LSan%20Tests%20(1)/41862/overview

Original change's description:
> Quick Answers: Fix timing issue on view destruction
>
> Call the UI controller on view destruction to avoid possible timing
> issue.
>
> ~~Bug: 1299225~~
> Test: Run existing tests
> Change-Id: Ice5a7a13324b3b68442bd91073f513c535f51c15
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499463
> Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
> Commit-Queue: Yue Li <updowndota@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#976595}

~~Bug: 1299225~~
Change-Id: Id320ae4a7a3342ed668c67c0e3baacb293fa668e
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3500513
Auto-Submit: Sergey Poromov <poromov@chromium.org>

Owners-Override: Sergey Poromov <poromov@chromium.org>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/heads/main@{#976677}

[modify]
https://crrev.com/f9beeea17c09e39c8187caa67b938a1688829d0b/chrome/browser/ui/quick_answers/ui/user_consent_view.cc
[modify]
https://crrev.com/f9beeea17c09e39c8187caa67b938a1688829d0b/chrome/browser/ui/quick_answers/ui/quick_answers_view.cc
[modify]
https://crrev.com/f9beeea17c09e39c8187caa67b938a1688829d0b/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify]
https://crrev.com/f9beeea17c09e39c8187caa67b938a1688829d0b/chrome/browser/ui/quick_answers/test/chrome_quick_answers_test_base.cc
[modify]
https://crrev.com/f9beeea17c09e39c8187caa67b938a1688829d0b/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc

Comment 22 by ellyj...@chromium.org on Wed, Mar 2, 2022, 11:32 AM EST

Status: Assigned (was: Fixed)

The ASAN test failure is caused by the View outliving the Controller, being unaware the Controller has been deallocated, and trying to call a method on it. It is deeply unsafe for the Controller to hold raw pointers to Views (which it does not control the lifetime of) and for Views to hold raw pointers to the Controller (which it does not control the lifetime of).

I *strongly* recommend having the Views hold references to the Controller as WeakPtrs, or (if that doesn't work) having the Controller hold references to Views via ViewTracker, which provides sort of the same functionality. Doing manual pointer invalidation is fraught with peril.

Comment 23 by updowndota@google.com on Thu, Mar 3, 2022, 12:36 AM EST

Status: Started (was: Assigned)

Working on a change with the ViewTracker/WeakPtrs approach.

Comment 24 by Git Watcher on Thu, Mar 3, 2022, 2:18 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d

commit 616c160eb7ee8ab538f274b651e5ce67a5ea4f8d
Author: Yue Li <updowndota@google.com>
Date: Thu Mar 03 19:17:49 2022

Quick Answers: Pass WeakPtr instead of raw pointer of UI controller

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: Ifb2236273a3c468fe9a16955bbc2843962595a24
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501322
Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
Commit-Queue: Yue Li <updowndota@chromium.org>

Cr-Commit-Position: refs/heads/main@{#977252}

[modify]

[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/ui/user_consent_view.cc
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/ui/quick_answers_view.h
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/ui/user_consent_view.h
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/ui/quick_answers_view.cc
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc
[modify]
https://crrev.com/616c160eb7ee8ab538f274b651e5ce67a5ea4f8d/chrome/browser/ui/quick_answers/ui/quick_answers_view_unittest.cc

Comment 25 by Git Watcher on Thu, Mar 3, 2022, 8:00 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/24747a485174e78bf8b2b8a6269c8ca8d0a529cb

commit 24747a485174e78bf8b2b8a6269c8ca8d0a529cb
Author: Yue Li <updowndota@google.com>
Date: Fri Mar 04 00:59:50 2022

Quick Answers: Use ViewTracker to avoid issue on view destruction

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: I368fdd5c17cc1ae1658ab870e72a613c1b09c2e3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501531
Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
Commit-Queue: Yue Li <updowndota@chromium.org>
Cr-Commit-Position: refs/heads/main@{#977433}

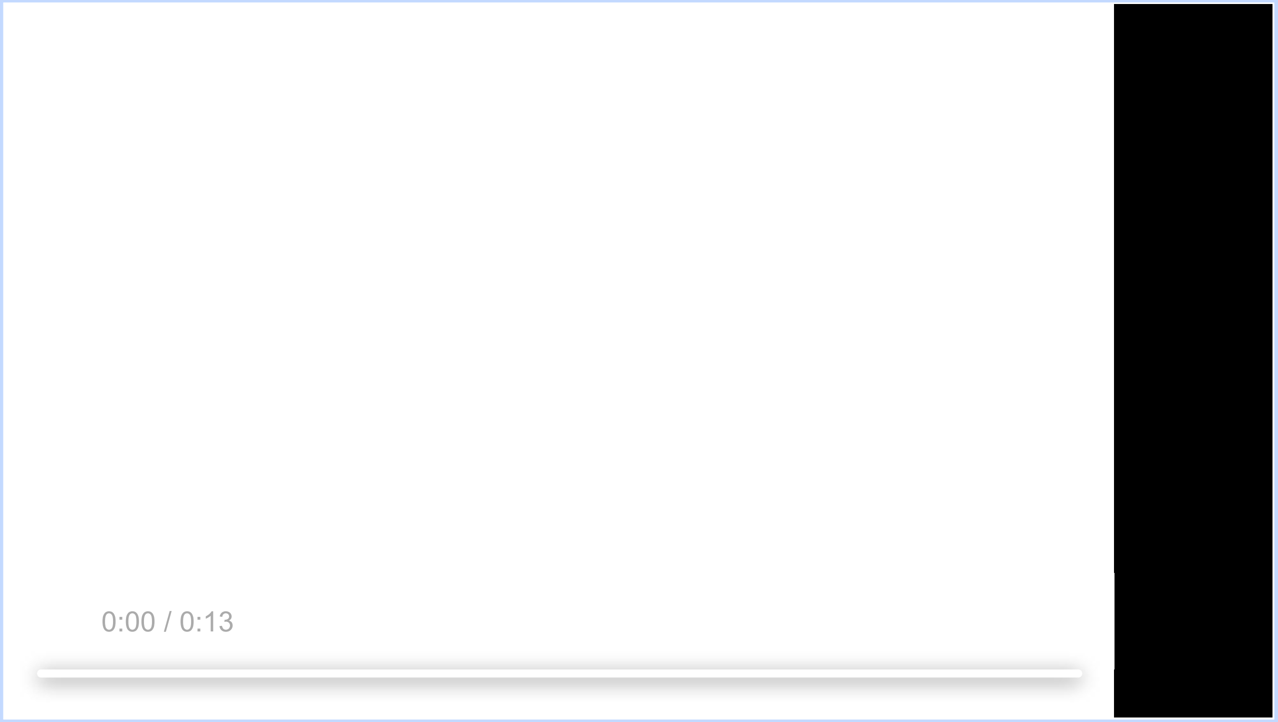
[modify]
https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_ui_controller_unittest.cc
[modify]
https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_controller_impl.cc
[modify]
https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify]
https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc
[modify]
https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_cont

https://crrev.com/24747a485174e78bf8b2b8a6269c8ca8d0a529cb/chrome/browser/ui/quick_answers/quick_answers_controller_unittest.cc

Comment 26 by chrom...@gmail.com on Thu, Mar 3, 2022, 11:09 PM EST

Thanks for the fix!

screen.webm
1.3 MB View Download



Comment 27 by updowndota@google.com on Fri, Mar 4, 2022, 1:19 AM EST

Status: Fixed (was: Started)

Comment 28 by sheriffbot on Fri, Mar 4, 2022, 12:42 PM EST

Labels: reward-topanel

Comment 29 by sheriffbot on Fri, Mar 4, 2022, 1:41 PM EST

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

Comment 30 by sheriffbot on Fri, Mar 4, 2022, 2:02 PM EST

Labels: Merge-Request-100 Merge-Request-98 Merge-Request-99

Requesting merge to extended stable M98 because latest trunk commit (977433) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (977433) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (977433) appears to be after beta branch point (972766).

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

Comment 31 by dgagnon@google.com on Fri, Mar 4, 2022, 2:52 PM EST

updowndota@ - Can you confirm if this change needs to be merged to release branches (see comment #30)?

Comment 32 by sheriffbot on Fri, Mar 4, 2022, 8:04 PM EST

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 is already shipping to beta.

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

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

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

Comment 33 by sheriffbot on Fri, Mar 4, 2022, 8:04 PM EST

Labels: -Merge-Request-99 Merge-Review-99

Merge review required: M99 is already shipping to stable.

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

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

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

Comment 34 by sheriffbot on Fri, Mar 4, 2022, 8:04 PM EST

Labels: -Merge-Request-98 Merge-Review-98

Merge review required: M98 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:

1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines

- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

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

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

Comment 35 by updowndota@google.com on Fri, Mar 4, 2022, 8:10 PM EST

Yes I think we should try to merge to earlier branches if possible. This is a long existing issue, though it rarely happens.

Comment 36 by ceb@google.com on Mon, Mar 7, 2022, 12:18 PM EST

Labels: -Merge-Review-99 Merge-Approved-99

Merge approved for M99. Please submit asap, we'll be cutting another stable RC mid-week.

Comment 37 by Git Watcher on Tue, Mar 8, 2022, 10:54 AM EST

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/0358cfdcc41283e02a0d2d03450e0b4ff5198da2

commit 0358cfdcc41283e02a0d2d03450e0b4ff5198da2
Author: Yue Li <updowndota@google.com>
Date: Tue Mar 08 15:53:37 2022

[M99 Merge] Quick Answers: Pass WeakPtr instead of raw pointer of UI controller

(cherry picked from commit 616c160eb7ee8ab538f274b651e5ce67a5ea4f8d)

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: Ifb2236273a3c468fe9a16955bbc2843962595a24
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501322
Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
Commit-Queue: Yue Li <updowndota@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977252}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508255
Auto-Submit: Yue Li <updowndota@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/branch-heads/4844@{#1010}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]

https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/ui/user_consent_view.cc
[modify]

[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/ui/quick_answers_view.h
[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/ui/user_consent_view.h
[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/ui/quick_answers_view.cc
[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc
[modify]
https://crrev.com/0358cfdcc41283e02a0d2d03450e0b4ff5198da2/chrome/browser/ui/quick_answers/ui/quick_answers_view_unittest.cc

Comment 38 by sheriffbot on Tue, Mar 8, 2022, 10:59 AM EST

Labels: LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 39 by Git Watcher on Tue, Mar 8, 2022, 2:31 PM EST

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b

commit d0302488d12d1aa6b0ff3fc51d3641f632f89b4b
Author: Yue Li <updowndota@google.com>
Date: Tue Mar 08 19:29:57 2022

[M99 Merge] Quick Answers: Use ViewTracker to avoid issue on view destruction

(cherry picked from commit 24747a485174e78bf8b2b8a6269c8ca8d0a529cb)

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: I368fdd5c17cc1ae1658ab870e72a613c1b09c2e3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501531
Reviewed-by: Xiyuan Xia <xiyuan@chromium.org>
Commit-Queue: Yue Li <updowndota@chromium.org>

Cr-Original-Commit-Position: refs/heads/main@{#977433}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3509812
Reviewed-by: Avi Drissman <avi@chromium.org>

Reviewed-by: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/branch-heads/4844@{#1012}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify] https://crrev.com/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b/chrome/browser/ui/quick_answers/quick_answers_ui_controller_unittest.cc
[modify] https://crrev.com/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b/chrome/browser/ui/quick_answers/quick_answers_controller_impl.cc
[modify] https://crrev.com/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b/chrome/browser/ui/quick_answers/quick_answers_ui_controller.h
[modify] https://crrev.com/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b/chrome/browser/ui/quick_answers/quick_answers_ui_controller.cc
[modify] https://crrev.com/d0302488d12d1aa6b0ff3fc51d3641f632f89b4b/chrome/browser/ui/quick_answers/quick_answers_controller_unittest.cc

Comment 40 by dgagnon@google.com on Tue, Mar 8, 2022, 8:20 PM EST

Labels: -Merge-Review-100 Merge-Approved-100

Merge approved for M100

Comment 41 by rzanoni@google.com on Wed, Mar 9, 2022, 8:23 AM EST

Cc: rzanoni@google.com
Labels: LTS-Evaluating-96

Comment 42 by rzanoni@google.com on Thu, Mar 10, 2022, 3:34 AM EST

Labels: -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 43 by sheriffbot on Thu, Mar 10, 2022, 3:38 AM EST

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

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 44 by rzanoni@google.com on Thu, Mar 10, 2022, 3:57 AM EST

1. 2 CLs https://chromium-review.googlesource.com/q/topic:4664_1299225
2. Medium, needed to do a few changes for conflict resolution and build fixes, better to ask the author to review the changes
3. 99
4. Yes

4. Yes

Comment 45 by gmpritchard@google.com on Thu, Mar 10, 2022, 9:40 AM EST

Labels: -LTS-Merge-Candidate LTS-Merge-Delayed-96

Delaying approval while we check with author.

Comment 46 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 PM EST

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 47 by amyressler@chromium.org on Thu, Mar 10, 2022, 11:04 PM EST

Thank you for this report, Khalil. The VRP Panel has decided to award you $3,000 for this report given the unusual user interaction required to trigger this issue. Thank you for your efforts and reporting this issue to us!

Comment 48 by amyressler@google.com on Fri, Mar 11, 2022, 2:44 PM EST

Labels: -reward-unpaid reward-inprocess

Comment 49 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:25 PM EST

Labels: Release-1-M99

Comment 50 by gmpritchard@google.com on Mon, Mar 14, 2022, 11:30 AM EDT

Labels: -LTS-Merge-Review-96 -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 51 by sheriffbot on Mon, Mar 14, 2022, 12:24 PM EDT

Cc: ceb@google.com dgagnon@google.com

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

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

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

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

Comment 52 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT

Labels: CVE-2022-0977 CVE_description-missing

Comment 53 by Git Watcher on Thu, Mar 17, 2022, 10:33 AM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/650d48c86955c9e7172612810022c2b1ff0129d5

commit 650d48c86955c9e7172612810022c2b1ff0129d5
Author: Yue Li <updowndota@google.com>
Date: Thu Mar 17 14:32:10 2022

[M96-LTS] Quick Answers: Pass WeakPtr instead of raw pointer of UI controller

M96 merge issues:
quick_answers_ui_controller.h:
- conflicting includes
quick_answers_view.cc:
- On QuickAnswersView::AddSettingsButton, settings_button_->SetImage()
isn't called on main. Kept the call and changed BindRepeating() args.
quick_answers_view.h:
- conflicting includes
quick_answers_view_unittest.cc:
- conflicting includes
user_consent_view.h:
- conflicting includes

(cherry picked from commit 616c160eb7ee8ab538f274b651e5ce67a5ea4f8d)

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: Ifb2236273a3c468fe9a16955bbc2843962595a24
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501322
Commit-Queue: Yue Li <updowndota@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977252}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3512634
Reviewed-by: Yue Li <updowndota@chromium.org>
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/4664@{#1539}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/quick_answers_ui_controller.cc
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/ui/quick_answers_view.h
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/ui/quick_answers_view_unittest.cc
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/ui/user_consent_view.h
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/ui/user_consent_view.cc
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/quick_answers_ui_controller.h
[modify] https://crrev.com/650d48c86955c9e7172612810022c2b1ff0129d5/ash/quick_answers/ui/quick_answers_view.cc

Comment 54 by Git Watcher on Thu, Mar 17, 2022, 12:42 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/08e5c10085e2e87b8c3b901ffa11293550140140

commit 08e5c10085e2e87b8c3b901ffa11293550140140
Author: Yue Li <updowndota@google.com>
Date: Thu Mar 17 16:41:41 2022

[M96-LTS] Quick Answers: Use ViewTracker to avoid issue on view destruction

M96 merge issues:
  quick_answers_controller_impl.cc:
  - conflict on call to OnConsentResult() (not prefixed with
  ash namespace on main) in MaybeDismissQuickAnswersConsent()
  - conflicting comments in ShowUserConsent()
  quick_answers_ui_controller.cc:
  - Defaulted QuickAnswersUiController destructor on main, kept
  M96 destructor
  - user_notice_view_ not present on main kept M96 related code
  in CreateQuickAnswersView, UpdateQuickAnswersBounds
  and CreateUserConsentView
  quick_answers_ui_controller.h:
  - is_showing_user_notice_view, notice_view_for_testing not
  present in main, kept
  quick_answers_ui_controller_unittest.cc:
  - TearDownWhileQuickAnswersViewShowing: CreateAndShowBasicMenu not
  present in M96, removed
  - is_showing_user_notice_view in TearDownWhileNoticeViewShowing not
  present in main, kept

(cherry picked from commit 24747a485174e78bf8b2b8a6269c8ca8d0a529cb)

~~Bug: 1299225~~
Test: Run existing tests
Change-Id: I368fdd5c17cc1ae1658ab870e72a613c1b09c2e3
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501531
Commit-Queue: Yue Li <updowndota@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977433}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3512814
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/4664@{#1541}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_controller_impl.cc
[modify]
https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_ui_controller.cc
[modify]
https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_ui_controller_unittest.cc
[modify]
https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_controller_unittest.cc
[modify]
https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_ui_controller.h

https://crrev.com/08e5c10085e2e87b8c3b901ffa11293550140140/ash/quick_answers/quick_answers_ui_controller.h

Comment 55 by rzanoni@google.com on Fri, Mar 18, 2022, 4:51 AM EDT

Labels: -LTS-Merge-Approved-96 LTS-Merge-Merged-96

Comment 56 by sheriffbot on Fri, Mar 18, 2022, 12:20 PM EDT

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

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

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

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

Comment 57 by sheriffbot on Fri, Jun 10, 2022, 1:31 PM EDT

Labels: -Restrict-View-SecurityNotify allpublic

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

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

Comment 58 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT

Labels: CVE_description-submitted -CVE_description-missing

Comment 59 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:16 PM EDT

Labels: -CVE_description-missing --CVE_description-missing