☆ Starred by 3 users

| | |
|---|---|
| **Owner:** | krist...@chromium.org |
| **CC:** | carlosil@chromium.org<br>ellyj...@chromium.org<br>mac-bugs-priority@chromium.org |
| **Status:** | Fixed *(Closed)* |
| **Components:** | UI>Browser>Sharing |
| **Modified:** | Jul 29, 2022 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | 2 |
| **NextAction:** | ---- |
| **OS:** | Mac |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
reward-5000
Hotlist-Merge-Approved
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
M-98
Target-98
FoundIn-97
connect-backlog
Security_Impact-Extended
Connect-DesktopShareHub
LTS-NotApplicable-96
connect-iteration-17
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1127

### Issue 1291891: Uaf in qrcode_generator::QRCodeGeneratorBubbleController::OnBubbleClosed

Reported by echo1...@msn.cn on Fri, Jan 28, 2022, 3:28 AM EST

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/97.0.4692.99 Safari/537.36

Steps to reproduce the problem:
1. open chromium on Mac M1 with the following command: ./chromium --user-data-dir=./tmp http://127.0.0.1:8080 (the ip address is not necessary to be valid)
2. right-click to show QR code
3. repeat step 2; if the former QR code not closed when clicking, a Uaf would be triggered
4. close tab

What is the expected behavior?

What went wrong?

```
=================================================================
==12746==ERROR: AddressSanitizer: heap-use-after-free on address 0x6030002ef438 at pc 0x00015da27683 bp 0x000306338980 sp 0x000306338978
WRITE of size 1 at 0x6030002ef438 thread T0
==12746==WARNING: Can't read from symbolizer at fd 101
==12746==WARNING: Can't read from symbolizer at fd 102
==12746==WARNING: Can't read from symbolizer at fd 103
==12746==WARNING: Can't read from symbolizer at fd 104
==12746==WARNING: Failed to use and restart external symbolizer!
    #0 0x15da27682 in qrcode_generator::QRCodeGeneratorBubbleController::OnBubbleClosed()+0x52 (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x1803b682) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #1 0x15e1eb8ab in non-virtual thunk to qrcode_generator::QRCodeGeneratorBubble::WindowClosing()+0x10b (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x187ff8ab) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #2 0x15c7594f4 in views::Widget::OnNativeWidgetDestroying()+0x924 (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x16d6d4f4) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #3 0x15c800c48 in non-virtual thunk to views::NativeWidgetMacNSWindowHost::OnWindowWillClose()+0xc8 (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x16e14c48) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #4 0x158bb58b6 in remote_cocoa::NativeWidgetNSWindowBridge::OnWindowWillClose()+0xf6 (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x131c98b6) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #5 0x158bc3f3b in -[ViewsNSWindowDelegate windowWillClose:]+0x30b (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium

Framework:x86_64+0x131d7f3b) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #6 0x7ff806a9e1be in __CFNOTIFICATIONCENTER_IS_CALLING_OUT_TO_AN_OBSERVER__+0xb
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x751be) (BuildId:
```

```
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x751be) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #7 0x7ff806b3abd4 in ___CFXRegistrationPost_block_invoke+0x30
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x111bd4) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #8 0x7ff806b3ab45 in _CFXRegistrationPost+0x1ef
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x111b45) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #9 0x7ff806a6fe99 in _CFXNotificationPost+0x322
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x46e99) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #10 0x7ff8077de1bd in -[NSNotificationCenter postNotificationName:object:userInfo:]+0x51
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0x91bd) (BuildId:
d97bfba6881833c6a51166f5c432fbd732000000020000000100000000020c00)
    #11 0x7ff809c8a02e in -[NSWindow _finishClosingWindow]+0x77
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x8cc02e) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000020000000100000000020c00)
    #12 0x7ff80971648e in -[NSWindow _close]+0x14f
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x35848e) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000020000000100000000020c00)
    #13 0x158bb5c87 in remote_cocoa::NativeWidgetNSWindowBridge::OnWindowWillClose()+0x4c7
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x131c9c87) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #14 0x158bc3f3b in -[ViewsNSWindowDelegate windowWillClose:]+0x30b (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x131d7f3b) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #15 0x7ff806a9e1be in __CFNOTIFICATIONCENTER_IS_CALLING_OUT_TO_AN_OBSERVER__+0xb
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x751be) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #16 0x7ff806b3abd4 in ___CFXRegistrationPost_block_invoke+0x30
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x111bd4) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #17 0x7ff806b3ab45 in _CFXRegistrationPost+0x1ef
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x111b45) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #18 0x7ff806a6fe99 in _CFXNotificationPost+0x322
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x46e99) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000020000000100000000020c00)
    #19 0x7ff8077de1bd in -[NSNotificationCenter postNotificationName:object:userInfo:]+0x51
(/System/Library/Frameworks/Foundation.framework/Versions/C/Foundation:x86_64+0x91bd) (BuildId:
d97bfba6881833c6a51166f5c432fbd732000000020000000100000000020c00)
    #20 0x7ff809c8a02e in -[NSWindow _finishClosingWindow]+0x77
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x8cc02e) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000020000000100000000020c00)
    #21 0x7ff80971648e in -[NSWindow _close]+0x14f
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x35848e) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000020000000100000000020c00)
    #22 0x15692b290 in base::internal::Invoker<base::internal::BindState<base::ScopedTypeRef<void () block_pointer,
base::mac::internal::ScopedBlockTraits<void () block_pointer> > >, void ()>::RunOnce(base::internal::BindStateBase*)+0x50
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium

Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x10f3f290) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #23 0x1532d834f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)+0x34f (/Users/krace/fuzz/chromium/asan
    #23 0x1532d834f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)+0x34f (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd8ec34f) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #24 0x15331cbac in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*)+0x4dc (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd930bac) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #25 0x15331c3a6 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x126
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd9303a6) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #26 0x15331d871 in non-virtual thunk to
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x11
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd931871) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #27 0x1534019f8 in base::MessagePumpCFRunLoopBase::RunWork()+0x188 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xda159f8) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #28 0x1533eeee9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xda02ee9) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #29 0x153400315 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0x175
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xda14315) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #30 0x7ff806aa8c07 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7fc07) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)
    #31 0x7ff806aa8b6f in __CFRunLoopDoSource0+0xb3
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7fb6f) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)
    #32 0x7ff806aa88e2 in __CFRunLoopDoSources0+0xf1
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7f8e2) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)
    #33 0x7ff806aa72fe in __CFRunLoopRun+0x380
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7e2fe) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)
    #34 0x7ff806aa68a8 in CFRunLoopRunSpecific+0x236
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7d8a8) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)
    #35 0x7ff80fb324f0 in RunCurrentEventLoopInMode+0x123
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_6
4+0x324f0) (BuildId: c538aa787afd3f8a8fdb1fc2acde6b3f32000000200000000100000000020c00)
    #36 0x7ff80fb32246 in ReceiveNextEventCommon+0x24a
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_6
4+0x32246) (BuildId: c538aa787afd3f8a8fdb1fc2acde6b3f32000000200000000100000000020c00)
    #37 0x7ff80fb31fe4 in _BlockUntilNextEventMatchingListInModeWithFilter+0x45
(/System/Library/Frameworks/Carbon.framework/Versions/A/Frameworks/HIToolbox.framework/Versions/A/HIToolbox:x86_6

4+0x31fe4) (BuildId: c538aa787afd3f8a8fdb1fc2acde6b3f32000000200000000100000000020c00)
    #38 0x7ff8093fcd87 in _DPSNextEvent+0x375
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x3cd87) (BuildId:
```

```
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x3ed87) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000200000000100000000020c00)
    #39 0x7ff8093fb3f3 in -[NSApplication(NSEvent) _nextEventMatchingEventMask:untilDate:inMode:dequeue:]+0x582
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x3d3f3) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000200000000100000000020c00)
    #40 0x152154b42 in __71-[BrowserCrApplication
nextEventMatchingMask:untilDate:inMode:dequeue:]_block_invoke+0x192 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc768b42) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #41 0x1533eeee9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xda02ee9) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #42 0x1521546da in -[BrowserCrApplication nextEventMatchingMask:untilDate:inMode:dequeue:]+0x32a
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc7686da) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #43 0x7ff8093ed918 in -[NSApplication run]+0x249
(/System/Library/Frameworks/AppKit.framework/Versions/C/AppKit:x86_64+0x2f918) (BuildId:
a737ebe63a9c32f3b9755ce0ef6313e432000000200000000100000000020c00)
    #44 0x1534033ba in base::MessagePumpNSApplication::DoRun(base::MessagePump::Delegate*)+0x3da
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xda173ba) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #45 0x1533ff0f8 in base::MessagePumpCFRunLoopBase::Run(base::MessagePump::Delegate*)+0x208
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xda130f8) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #46 0x15331df56 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool,
base::TimeDelta)+0x2a6 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd931f56) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #47 0x15325103c in base::RunLoop::Run(base::Location const&)+0x4ac (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd86503c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #48 0x14a3324e2 in content::BrowserMainLoop::RunMainMessageLoop()+0x2c2 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x49464e2) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #49 0x14a336b21 in content::BrowserMainRunnerImpl::Run()+0x31 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x494ab21) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #50 0x14a32be95 in content::BrowserMain(content::MainFunctionParams)+0x2a5 (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x493fe95) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #51 0x151fa8dda in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*)+0x26a (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc5bcdda) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #52 0x151fabbb3 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)+0xb43
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc5bfbb3) (BuildId:

4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #53 0x151faae37 in content::ContentMainRunnerImpl::Run()+0x467 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc5bee37) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #54 0x151fa777b in content::RunContentProcess(content::ContentMainParams, content::ContentMainRunner*)+0x170b
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc5bb77b) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #55 0x151fa7eed in content::ContentMain(content::ContentMainParams)+0x12d (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc5bbeed) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #56 0x1459f0a91 in ChromeMain+0x231 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x4a91) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #57 0x100ed3bb5 in main+0x205 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/MacOS/Chromium:x86_64+0x100000bb5) (BuildId:
4c4c445355553144a1fc3447960c0cb42400000010000000000b0a0000010c00)
    #58 0x2013b94fd  (/usr/lib/dyld:x86_64+0x54fd) (BuildId:
7de33963bbc53996ba6ef1d562c17c95320000000200000001000000000020c00)

0x6030002ef438 is located 24 bytes inside of 32-byte region [0x6030002ef420,0x6030002ef440)
freed by thread T0 here:
    #0 0x109904019 in __asan_memmove+0x1ce9 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/MacOS/libclang_rt.asan_osx_dynamic.dylib:x86_64+0x47019) (BuildId:
b4732162098e3d0f8e0b461cd4a2204324000000100000000070a0000010b00)
    #1 0x1532cb695 in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0xa5 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df695) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #2 0x1532cb64c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0x5c (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df64c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #3 0x1532cb62d in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0x3d (/Users/krace/fuzz/chromium/asan-mac-

release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df62d) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #4 0x1532cb64c in std::__1::__tree<std::__1::__value_type<void const*,
    #4 0x1532cb64c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0x5c (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df64c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #5 0x1532cb64c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0x5c (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df64c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #6 0x1532cb64c in std::__1::__tree<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::__map_value_compare<void const*, std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > >,
std::__1::less<void const*>, true>, std::__1::allocator<std::__1::__value_type<void const*,
std::__1::unique_ptr<base::SupportsUserData::Data, std::__1::default_delete<base::SupportsUserData::Data> > > >
>::destroy(std::__1::__tree_node<std::__1::__value_type<void const*, std::__1::unique_ptr<base::SupportsUserData::Data,
std::__1::default_delete<base::SupportsUserData::Data> > >, void*>*)+0x5c (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8df64c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #7 0x1532cae63 in base::SupportsUserData::~SupportsUserData()+0x1d3 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xd8dee63) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #8 0x14b5a21e2 in content::WebContentsImpl::~WebContentsImpl()+0x1852 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x5bb61e2) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #9 0x14b5a455d in content::WebContentsImpl::~WebContentsImpl()+0xd (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x5bb855d) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #10 0x15d4a691a in TabStripModel::SendDetachWebContentsNotifications(TabStripModel::DetachNotifications*)+0xf9a
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17aba91a) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #11 0x15d4af9a7 in TabStripModel::CloseTabs(base::span<content::WebContents* const, 18446744073709551615ul>,
unsigned int)+0xac7 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17ac39a7) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #12 0x15d4b100e in TabStripModel::CloseWebContentsAt(int, unsigned int)+0x1ae (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17ac500e) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)

    #13 0x15d35c501 in chrome::CloseWebContents(Browser*, content::WebContents*, bool)+0x51
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17950501) (BuildId:
```

```
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17970501) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #14 0x14b62cf04 in content::WebContentsImpl::Close(content::RenderViewHost*)+0x224
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x5c40f04) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #15 0x14b1de8ea in base::internal::Invoker<base::internal::BindState<void (content::RenderViewHostImpl::*)(),
base::WeakPtr<content::RenderViewHostImpl> >, void ()>::RunOnce(base::internal::BindStateBase*)+0x1ba
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x57f28ea) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #16 0x148d9159a in blink::mojom::LocalMainFrame_ClosePage_ForwardToCallback::Accept(mojo::Message*)+0x11a
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x33a559a) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #17 0x1538d237c in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)+0xb6c
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xdee637c) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #18 0x1538e06a4 in mojo::MessageDispatcher::Accept(mojo::Message*)+0x3f4 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xdef46a4) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #19 0x1538d6694 in mojo::InterfaceEndpointClient::HandleIncomingMessage(mojo::Message*)+0x154
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xdeea694) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #20 0x155577f2d in IPC::(anonymous
namespace)::ChannelAssociatedGroupController::AcceptOnEndpointThread(mojo::Message)+0x39d
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xfb8bf2d) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #21 0x155571b9c 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*)+0x16c (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xfb85b9c) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #22 0x1532d834f in base::TaskAnnotator::RunTaskImpl(base::PendingTask&)+0x34f (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd8ec34f) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #23 0x15331cbac in
base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::Lazy
Now*)+0x4dc (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd930bac) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #24 0x15331c3a6 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x126
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd9303a6) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #25 0x15331d871 in non-virtual thunk to

base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()+0x11
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd931871) (BuildId:
```

```
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xd931871) (BuildId:
4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #26 0x1534019f8 in base::MessagePumpCFRunLoopBase::RunWork()+0x188 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xda159f8) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #27 0x1533eeee9 in base::mac::CallWithEHFrame(void () block_pointer)+0x9 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xda02ee9) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #28 0x153400315 in base::MessagePumpCFRunLoopBase::RunWorkSource(void*)+0x175
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xda14315) (BuildId:
4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #29 0x7ff806aa8c07 in __CFRUNLOOP_IS_CALLING_OUT_TO_A_SOURCE0_PERFORM_FUNCTION__+0x10
(/System/Library/Frameworks/CoreFoundation.framework/Versions/A/CoreFoundation:x86_64+0x7fc07) (BuildId:
f56186e256053c5c9063c14ba1ba950c32000000200000000100000000020c00)

previously allocated by thread T0 here:
    #0 0x109903ed0 in __asan_memmove+0x1ba0 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/MacOS/libclang_rt.asan_osx_dynamic.dylib:x86_64+0x46ed0) (BuildId:
b4732162098e3d0f8e0b461cd4a220432400000010000000000070a0000010b00)
    #1 0x1520d0907 in operator new(unsigned long)+0x27 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc6e4907) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #2 0x15da272ec in qrcode_generator::QRCodeGeneratorBubbleController::Get(content::WebContents*)+0x3c
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x1803b2ec) (BuildId:
4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #3 0x15e255463 in sharing_hub::SharingHubIconView::UpdateImpl()+0xa3 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x18869463) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #4 0x15e0146f3 in PageActionIconController::UpdateAll()+0x73 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x186286f3) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #5 0x15deab572 in LocationBarView::Update(content::WebContents*)+0xc2 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x184bf572) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #6 0x15e48bfbd in ToolbarView::Update(content::WebContents*)+0x3d (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x18a9ffbd) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #7 0x15d2eca8d in Browser::OnActiveTabChanged(content::WebContents*, content::WebContents*, int, int)+0x30d
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17900a8d) (BuildId:
4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #8 0x15d2ebac7 in Browser::OnTabStripModelChanged(TabStripModel*, TabStripModelChange const&,
TabStripSelectionChange const&)+0x4d7 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x178ffac7) (BuildId: 4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #9 0x15d4a2bac in TabStripModel::InsertWebContentsAtImpl(int, std::__1::unique_ptr<content::WebContents,
std::__1::default_delete<content::WebContents> >, int, absl::optional<tab_groups::TabGroupId>)+0xc1c
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17ab6bac) (BuildId:

4c4c447a55553144a18c0e4270a72e2b240000001000000000b0a0000010c00)
    #10 0x15d4b5a18 in TabStripModel::AddWebContents(std::__1::unique_ptr<content::WebContents,
std::__1::default_delete<content::WebContents> >, int, ui::PageTransition, int
```

```
std::__1::default_delete<content::WebContents> >, int, ui::PageTransition, int,
absl::optional<tab_groups::TabGroupId>)+0x5f8 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17ac9a18) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #11 0x15d350c36 in Navigate(NavigateParams*)+0x2d26 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17964c36) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #12 0x15d485baf in StartupBrowserCreatorImpl::OpenTabsInBrowser(Browser*, chrome::startup::IsProcessStartup,
std::__1::vector<StartupTab, std::__1::allocator<StartupTab> > const&)+0x6ff (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17a99baf) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #13 0x15d48813d in StartupBrowserCreatorImpl::RestoreOrCreateBrowser(std::__1::vector<StartupTab,
std::__1::allocator<StartupTab> > const&, StartupBrowserCreatorImpl::BrowserOpenBehavior, unsigned int,
chrome::startup::IsProcessStartup, bool)+0x40d (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17a9c13d) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #14 0x15d484bb3 in StartupBrowserCreatorImpl::DetermineURLsAndLaunch(chrome::startup::IsProcessStartup)+0x7b3
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17a98bb3) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #15 0x15d4840be in StartupBrowserCreatorImpl::Launch(Profile*, chrome::startup::IsProcessStartup,
std::__1::unique_ptr<LaunchModeRecorder, std::__1::default_delete<LaunchModeRecorder> >)+0xee
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17a980be) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #16 0x15d47b8eb in StartupBrowserCreator::LaunchBrowser(base::CommandLine const&, Profile*, base::FilePath
const&, chrome::startup::IsProcessStartup, chrome::startup::IsFirstRun, std::__1::unique_ptr<LaunchModeRecorder,
std::__1::default_delete<LaunchModeRecorder> >)+0x13b (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17a8f8eb) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #17 0x15d47c6b6 in StartupBrowserCreator::LaunchBrowserForLastProfiles(base::CommandLine const&, base::FilePath
const&, chrome::startup::IsProcessStartup, chrome::startup::IsFirstRun, StartupProfileInfo, std::__1::vector<Profile*,
std::__1::allocator<Profile*> > const&)+0x3f6 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17a906b6) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #18 0x15d47ae26 in StartupBrowserCreator::ProcessCmdLineImpl(base::CommandLine const&, base::FilePath const&,
chrome::startup::IsProcessStartup, StartupProfileInfo, std::__1::vector<Profile*, std::__1::allocator<Profile*> >
const&)+0x16d6 (/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x17a8ee26) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #19 0x15d4795b6 in StartupBrowserCreator::Start(base::CommandLine const&, base::FilePath const&, StartupProfileInfo,
std::__1::vector<Profile*, std::__1::allocator<Profile*> > const&)+0x126 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x17a8d5b6) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #20 0x15218c273 in ChromeBrowserMainParts::PreMainMessageLoopRunImpl()+0x16b3
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc7a0273) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #21 0x15218a9cd in ChromeBrowserMainParts::PreMainMessageLoopRun()+0x5d (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc79e9cd) (BuildId:

4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
   #22 0x14a330170 in content::BrowserMainLoop::PreMainMessageLoopRun()+0x140 (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
```

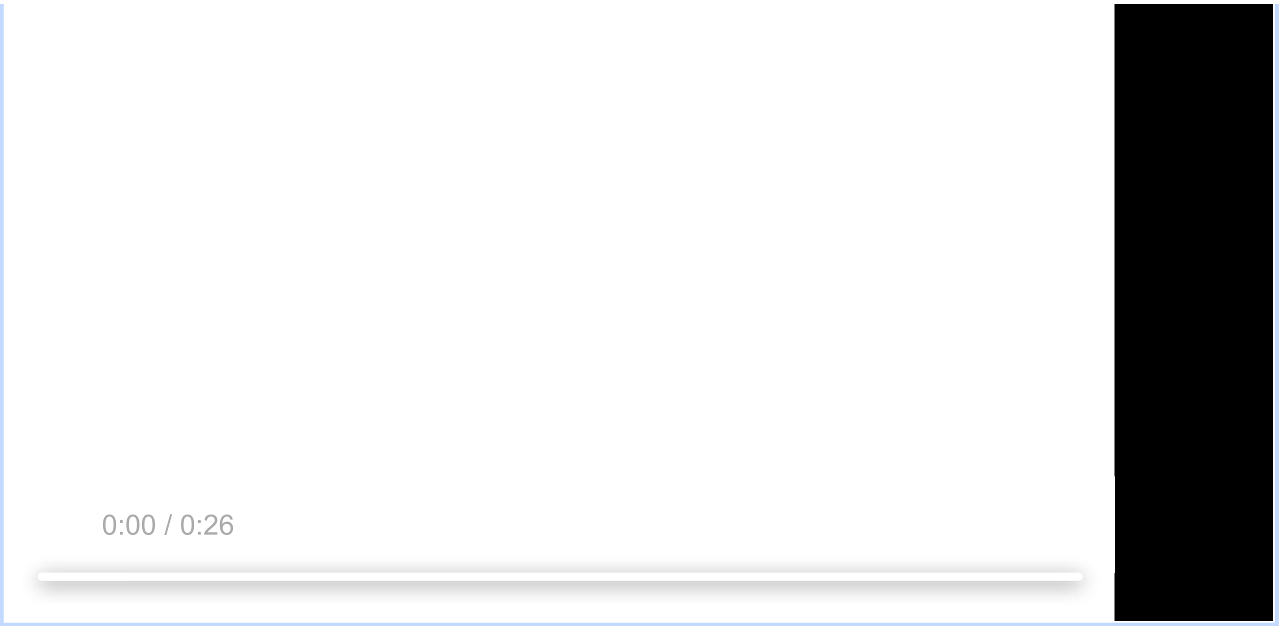
```
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x4944170) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #23 0x14b4fc94f in content::StartupTaskRunner::RunAllTasksNow()+0x13f (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x5b1094f) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #24 0x14a32f660 in content::BrowserMainLoop::CreateStartupTasks()+0x640 (/Users/krace/fuzz/chromium/asan-mac-
release-964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x4943660) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #25 0x14a3361bc in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams)+0x18c
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x494a1bc) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #26 0x14a32be47 in content::BrowserMain(content::MainFunctionParams)+0x257 (/Users/krace/fuzz/chromium/asan-
mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0x493fe47) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #27 0x151fa8dda in content::RunBrowserProcessMain(content::MainFunctionParams,
content::ContentMainDelegate*)+0x26a (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc5bcdda) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #28 0x151fabbb3 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams, bool)+0xb43
(/Users/krace/fuzz/chromium/asan-mac-release-964404/Chromium.app/Contents/Frameworks/Chromium
Framework.framework/Versions/100.0.4857.0/Chromium Framework:x86_64+0xc5bfbb3) (BuildId:
4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
    #29 0x151faae37 in content::ContentMainRunnerImpl::Run()+0x467 (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0xc5bee37) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)

SUMMARY: AddressSanitizer: heap-use-after-free (/Users/krace/fuzz/chromium/asan-mac-release-
964404/Chromium.app/Contents/Frameworks/Chromium Framework.framework/Versions/100.0.4857.0/Chromium
Framework:x86_64+0x1803b682) (BuildId: 4c4c447a55553144a18c0e4270a72e2b2400000010000000000b0a0000010c00)
in qrcode_generator::QRCodeGeneratorBubbleController::OnBubbleClosed()+0x52
Shadow bytes around the buggy address:
  0x1c060005de30: fd fd fd fd fa fa fd fd fd fd fa fa fd fd fd fd
  0x1c060005de40: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x1c060005de50: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x1c060005de60: 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00 00 fa
  0x1c060005de70: fa fa 00 00 00 fa fa fa 00 00 00 fa fa fa 00 00
=>0x1c060005de80: 00 00 fa fa fd fd fd[fd]fa fa fd fd fd fd fa fa
  0x1c060005de90: fd fd fd fa fa fa fd fd fd fa fa fa fd fd fd fd
  0x1c060005dea0: fa fa fd fd fd fd fa fa fd fd fd fd fa fa fd fd
  0x1c060005deb0: fd fd fa fa fd fd fd fd fa fa fd fd fd fd fa fa
  0x1c060005dec0: fd fd fd fd fa fa fd fd fd fd fa fa fd fd fd fd
  0x1c060005ded0: fa fa fd fd fd fd fa fa fd fd fd fd fa fa 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 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
==12746==ABORTING
Received signal 6
 [0x0001533c8f89]
 [0x00015316f133]
 [0x0001533c8d0b]
 [0x7ff8069f7e2d]
 [0x203e203e61746144]
 [0x7ff80692ed10]
 [0x000109929376]
 [0x000109928af4]
 [0x00010990c3a7]
 [0x00010990b63f]
 [0x00010990ca7b]
 [0x00015da27683]
 [0x00015e1eb8ac]
 [0x00015c7594f5]
 [0x00015c800c49]
 [0x000158bb58b7]
 [0x000158bc3f3c]
 [0x7ff806a9e1bf]
 [0x7ff806b3abd5]
 [0x7ff806b3ab46]
 [0x7ff806a6fe9a]
 [0x7ff8077de1be]
 [0x7ff809c8a02f]
 [0x7ff80971648f]
 [0x000158bb5c88]
 [0x000158bc3f3c]
 [0x7ff806a9e1bf]
 [0x7ff806b3abd5]
 [0x7ff806b3ab46]
 [0x7ff806a6fe9a]
 [0x7ff8077de1be]
 [0x7ff809c8a02f]
 [0x7ff80971648f]
 [0x00015692b291]
 [0x0001532d8350]
 [0x00015331cbad]
 [0x00015331c3a7]
 [0x00015331d872]

 [0x0001534019f9]
 [0x0001533eeeea]
 [0x00015340031c]
 [0x000153400316]
 [0x7ff806aa8c08]
 [0x7ff806aa8b70]
 [0x7ff806aa88e3]
 [0x7ff806aa72ff]
 [0x7ff806aa68a9]
 [0x7ff80fb324f1]
 [0x7ff80fb32247]
 [0x7ff80fb31fe5]
 [0x7ff8093fcd88]
 [0x7ff8093fb3f4]
 [0x000152154b43]
 [0x0001533eeeea]
 [0x0001521546db]
 [0x7ff8093ed919]
 [0x0001534033bb]
 [0x0001533ff0f9]
 [0x00015331df57]
 [0x00015325103d]
 [0x00014a3324e3]
 [0x00014a336b22]
 [0x00014a32be96]
 [0x000151fa8ddb]
 [0x000151fabbb4]
 [0x000151faae38]
 [0x000151fa777c]
 [0x000151fa7eee]
 [0x0001459f0a92]
 [0x000100ed3bb6]
 [0x0002013b94fe]
 [0x000000000003]
[end of stack trace]
[1]    12746 abort      ./Chromium
```

Did this work before? N/A

Chrome version: 97.0.4692.99  Channel: stable
OS Version: OS X 10.15.7

**uaf-reproduce.mp4**
1.2 MB  View  Download

[redacted]



Comment 1 by sheriffbot on Fri, Jan 28, 2022, 3:33 AM EST Project Member

**Labels:** external_security_report

Comment 2 by carlosil@chromium.org on Fri, Jan 28, 2022, 7:11 PM EST Project Member

~~Issue 1291892~~ has been merged into this issue.

Comment 3 by carlosil@chromium.org on Fri, Jan 28, 2022, 7:52 PM EST Project Member

**Labels:** Needs-Feedback

Thanks for the report, I tried reproducing in Windows, Linux, Chrome OS and Mac, but in all cases the first bubble closes on its own when right clicking to trigger the second one. Is there anything else you had to do to reproduce this?

Comment 4 by echo1...@msn.cn on Fri, Jan 28, 2022, 8:17 PM EST

Please try right-click immediately to show qrcode while the site is not entirely loaded. As in the video, I tried to click as chromium started yet this site was not ready to load. And I tried this only in Mac 13“ M1 with 16G RAM, the version of chromium is asan-964404.

Comment 5 by sheriffbot on Fri, Jan 28, 2022, 8:20 PM EST Project Member

**Cc:** carlosil@chromium.org
**Labels:** -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 6 by cthomp@chromium.org on Fri, Jan 28, 2022, 8:29 PM EST Project Member

On macOS ASAN r964565 I can't get the menu option to show QR code until after the page has loaded (in either the right-click menu or in the omnibox share menu). I also tried with https://httpbin.org/delay/10 (to force a consistent 10 second delay) and could not there either. It does show up on a new navigation if there already exists an active previous page, but then it behaves like it does when the page has already finished loading (right clicking again closes the bubble).

If this is triggerable, it seems like a very tight window, potentially only at browser startup, which seems like it might not be

If this is triggerable, it seems like a very tight window, potentially only at browser startup, which seems like it might not be exploitable.

Comment 7 by echo1...@msn.cn on Mon, Jan 31, 2022, 11:42 AM EST

asan with symbol

**asan.txt**
24.2 KB View Download

Comment 8 by xinghuilu@chromium.org on Tue, Feb 1, 2022, 3:32 PM EST Project Member

**Status:** Assigned (was: Unconfirmed)
**Owner:** krist...@chromium.org
**Cc:** ellyj...@chromium.org
**Labels:** Security_Severity-High FoundIn-97
**Components:** UI>Browser>Sharing

Thanks for the report! Similar to #c2 and #c6, I'm not able to reproduce either. The stack trace indicates some kind of race condition in the callback. There might be some corner cases that are hard to reproduce.

+kristipark@, I saw that there is currently an ongoing investigation on QRCodeGeneratorBubbleController in https://crbug.com/1278983. Could you take a look and see if this can be the same root cause? Thanks!

Also +ellyjones@, since you have dealt with CloseBubble UAF in the past (~~https://crbug.com/1249491~~), and you added the on_closing callback for QRCodeGeneratorBubbleController in https://crrev.com/c/2880111. Is there a possible scenario that unretained is not safe?

Comment 9 by sheriffbot on Tue, Feb 1, 2022, 3:40 PM EST Project Member

**Labels:** Security_Impact-Stable

Comment 10 by sheriffbot on Tue, Feb 1, 2022, 5:37 PM EST Project Member

**Labels:** -Security_Impact-Stable Security_Impact-Extended

Comment 11 by sheriffbot on Wed, Feb 2, 2022, 12:51 PM EST Project Member

**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 12 by sheriffbot on Wed, Feb 2, 2022, 1:11 PM EST Project Member

**Labels:** -Pri-2 Pri-1

Setting Pri-1 to match security severity High. 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 13 by sheriffbot on Fri, Feb 11, 2022, 12:21 PM EST Project Member

kristipark: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

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

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

Comment 14 by krist...@chromium.org on Mon, Feb 14, 2022, 4:46 PM EST Project Member

**Labels:** connect-backlog connect-iteration-17
**EstimatedDays:** 2

Comment 15 by krist...@chromium.org on Mon, Feb 14, 2022, 4:56 PM EST Project Member

**Labels:** Connect-DesktopShareHub

Comment 16 by echo1...@msn.cn on Sun, Feb 20, 2022, 9:53 PM EST

ping

Comment 17 by Git Watcher on Thu, Feb 24, 2022, 2:41 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7a9d15519436b530d3fd219b53741be8530d2217

commit 7a9d15519436b530d3fd219b53741be8530d2217
Author: Kristi Park <kristipark@chromium.org>
Date: Thu Feb 24 19:40:19 2022

[QrCodeGenerator] Check if dialog is already open and remove Unretained callback

In unusual cases where the QR code dialog is opened twice in succession
(e.g. during startup with a slow processor), both dialogs remain open
instead of closing the first. Therefore when the window is closed and
the dialogs are cleaned up, one tries to callback to an already
discarded controller.

Hence, check if the dialog is already open to prevent two dialogs from
appearing, and replace base::Unretained with weak_ptr for good measure.

~~Bug: 1291891~~
Change-Id: Iba04d20c7a4b9b715df19ea5d644e9061f3db90b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3489106
Reviewed-by: Elly Fong-Jones <ellyjones@chromium.org>
Commit-Queue: Kristi Park <kristipark@chromium.org>
Cr-Commit-Position: refs/heads/main@{#974742}

[modify]
https://crrev.com/7a9d15519436b530d3fd219b53741be8530d2217/chrome/browser/ui/qrcode_generator/qrcode_generator_bubble_controller.cc
[modify]
https://crrev.com/7a9d15519436b530d3fd219b53741be8530d2217/chrome/browser/ui/views/frame/browser_view.cc

https://crrev.com/7a9d15519436b530d3fd219b53741be8530d2217/chrome/browser/ui/views/frame/browser_view.cc
[modify]
https://crrev.com/7a9d15519436b530d3fd219b53741be8530d2217/chrome/browser/ui/qrcode_generator/qrcode_generator_bubble_controller.h

Comment 18 by krist...@chromium.org on Fri, Feb 25, 2022, 2:55 PM EST Project Member

**Status:** Fixed (was: Assigned)

Comment 19 by sheriffbot on Sun, Feb 27, 2022, 12:41 PM EST Project Member

**Labels:** reward-topanel

Comment 20 by sheriffbot on Sun, Feb 27, 2022, 1:40 PM EST Project Member

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

Comment 21 by sheriffbot on Sun, Feb 27, 2022, 2:00 PM EST Project Member

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

Requesting merge to stable M98 because latest trunk commit (974742) appears to be after stable branch point (950365).

Requesting merge to beta M99 because latest trunk commit (974742) appears to be after beta branch point (961656).

Requesting merge to dev M100 because latest trunk commit (974742) appears to be after dev branch point (972766).

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

Comment 22 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

**Labels:** -Merge-Request-100 Merge-Approved-100 Hotlist-Merge-Approved

Merge approved: your change passed merge requirements and is auto-approved for M100. Please go ahead and merge the CL to branch 4896 (refs/branch-heads/4896) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 23 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

**Labels:** -Merge-Request-99 Hotlist-Merge-Review Merge-Review-99

Merge review required: M99 has already been cut for stable release.

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

please 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 24 by sheriffbot on Sun, Feb 27, 2022, 2:01 PM EST Project Member

**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
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 25 by krist...@chromium.org on Mon, Feb 28, 2022, 4:38 PM EST Project Member

**Labels:** -Merge-Review-98 -Merge-Review-99

Removing M99 & M98 merge requests

Comment 26 by Git Watcher on Mon, Feb 28, 2022, 6:55 PM EST Project Member

**Labels:** -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/78be1c5b4615d380d1353df0d46d95068e848b18

commit 78be1c5b4615d380d1353df0d46d95068e848b18
Author: Kristi Park <kristipark@chromium.org>
Date: Mon Feb 28 23:54:13 2022

[M100][QrCodeGenerator] Check if dialog is already open and remove Unretained callback

In unusual cases where the QR code dialog is opened twice in succession
(e.g. during startup with a slow processor), both dialogs remain open
instead of closing the first. Therefore when the window is closed and
the dialogs are cleaned up, one tries to callback to an already
discarded controller.

Hence, check if the dialog is already open to prevent two dialogs from
appearing, and replace base::Unretained with weak_ptr for good measure.

appearing, and replace base::Unretained with weak_ptr for good measure.

(cherry picked from commit 7a9d15519436b530d3fd219b53741be8530d2217)

~~Bug: 1291891~~
Change-Id: Iba04d20c7a4b9b715df19ea5d644e9061f3db90b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3489106
Reviewed-by: Elly Fong-Jones <ellyjones@chromium.org>
Commit-Queue: Kristi Park <kristipark@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#974742}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3495397
Auto-Submit: Kristi Park <kristipark@chromium.org>
Commit-Queue: Elly Fong-Jones <ellyjones@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#163}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/78be1c5b4615d380d1353df0d46d95068e848b18/chrome/browser/ui/qrcode_generator/qrcode_generator_bubble_controller.cc
[modify]
https://crrev.com/78be1c5b4615d380d1353df0d46d95068e848b18/chrome/browser/ui/qrcode_generator/qrcode_generator_bubble_controller.h
[modify]
https://crrev.com/78be1c5b4615d380d1353df0d46d95068e848b18/chrome/browser/ui/views/frame/browser_view.cc

Comment 27 by amyressler@google.com on Thu, Mar 3, 2022, 5:23 PM EST Project Member

**Labels:** -reward-topanel reward-unpaid reward-5000

*** 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 28 by amyressler@chromium.org on Thu, Mar 3, 2022, 5:34 PM EST Project Member

Hello and thank you for your report. The VRP Panel has decided to award you $5,000 for this report. A member of our finance team will reach out to you soon to arrange payment. In the interim, please let us know the name, handle/tag, or other identifier you would like us to use in acknowledging you for reporting this issue. Thank you for your efforts and reporting this issue to us!

Comment 29 by echo1...@msn.cn on Fri, Mar 4, 2022, 8:41 AM EST

Thank you! Please credit anonymous.

Comment 30 by amyressler@google.com on Fri, Mar 4, 2022, 6:32 PM EST Project Member

**Labels:** -reward-unpaid reward-inprocess

Comment 31 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:58 PM EDT Project Member

**Labels:** Release-0-M100

Comment 32 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

**Labels:** CVE-2022-1127 CVE_description-missing

Comment 33 by gmpritchard@google.com on Thu, Mar 31, 2022, 11:50 AM EDT Project Member

**Labels:** LTS-Merge-Candidate

Comment 34 by gmpritchard@google.com on Thu, Mar 31, 2022, 11:52 AM EDT Project Member

**Labels:** -LTS-Merge-Candidate LTS-NotApplicable-96

Comment 35 by sheriffbot on Sat, Jun 4, 2022, 1:31 PM EDT Project Member

**Labels:** -Restrict-View-SecurityNotify allpublic

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

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

Comment 36 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

**Labels:** CVE_description-submitted -CVE_description-missing

Comment 37 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

**Labels:** -CVE_description-missing --CVE_description-missing

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy