Starred by 5 users

Owner:	na...@chromium.org
CC:	olesiamarukhno@google.com sporeba@google.com a...@chromium.org engedy@chromium.org benmason@chromium.org dullweber@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Bubbles>PageInfo
Modified:	Oct 24, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Merge-na
reward-0
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
Via-Wizard-Security
CVE_description-submitted
M-91
Target-91
external_security_report
merge-merged-4430
merge-merged-90
FoundIn-91
merge-merged-4472
merge-merged-91
LTS-Merged-90
LTS-Security-90
merge-merged-4515
merge-merged-92
LTS-Size-Small
LTS-Complexity-Minimal
Release-1-M92

Issue 1218468: heap use after free in ChromePageInfoDelegate::OpenConnectionHelpCenterPage

Reported by wxhu...@gmail.com on Thu, Jun 10, 2021, 12:45 PM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36

Steps to reproduce the problem:
1.we can see the bug at https://bugs.chromium.org/p/chromium/issues/detail?id=1212498

and its browser_test in https://chromium.googlesource.com/chromium/src/+/9f8ca0e35834223cb58ce777c9ccd49e903e7434%5E%21/#F0
2. then i see the function ChromePageInfoDelegate::OpenConnectionHelpCenterPage,
it use the web_contents, and it has no webcontentobserver
3. so I think the bug pattern is smiliar, I try to write the unittest, and it shows that there has a use after free bug.

```
=================================================================
==30315==ERROR: AddressSanitizer: heap-use-after-free on address 0x61e0000a7480 at pc 0x55c83d067a9d bp 0x7ffcc9410990 sp 0x7ffcc9410988
READ of size 8 at 0x61e0000a7480 thread T0 (browser_tests)
    #0 0x55c83d067a9c in ChromePageInfoDelegate::OpenConnectionHelpCenterPage(ui::Event const&)
chrome/browser/ui/page_info/chrome_page_info_delegate.cc:177:18
    #1 0x55c81cc605dc in ChromePageInfoDelegateTest_OpenConnectionHelpCenterPageAfterWebContentsClosed_Test::RunTestOnMainThread()
chrome/browser/ui/page_info/chrome_page_info_delegate_browser_test.cc:92:10
    #2 0x55c83267374c in content::BrowserTestBase::ProxyRunTestOnMainThreadLoop() content/public/test/browser_test_base.cc:849:7
    #3 0x55c832677304 in Invoke<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:509:12
    #4 0x55c832677304 in MakeItSo<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:648:12
    #5 0x55c832677304 in RunImpl<void (content::BrowserTestBase::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserTestBase> >, 0UL>
base/bind_internal.h:721:12
    #6 0x55c832677304 in base::internal::Invoker<base::internal::BindState<void (content::BrowserTestBase::*)(),
base::internal::UnretainedWrapper<content::BrowserTestBase> >, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #7 0x55c830953dac in Run base/callback.h:98:12
    #8 0x55c830953dac in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome/browser/chrome_browser_main.cc:1733:38
    #9 0x55c8309514b5 in ChromeBrowserMainParts::PreMainMessageLoopRun() chrome/browser/chrome_browser_main.cc:1064:18
    #10 0x55c82699ae20 in content::BrowserMainLoop::PreMainMessageLoopRun() content/browser/browser_main_loop.cc:949:28
    #11 0x55c8269a1174 in Invoke<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:509:12
    #12 0x55c8269a1174 in MakeItSo<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:648:12
    #13 0x55c8269a1174 in RunImpl<int (content::BrowserMainLoop::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserMainLoop> >, 0UL>
base/bind_internal.h:721:12
    #14 0x55c8269a1174 in base::internal::Invoker<base::internal::BindState<int (content::BrowserMainLoop::*)(),
base::internal::UnretainedWrapper<content::BrowserMainLoop> >, int ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #15 0x55c827ce535b in Run base/callback.h:98:12
    #16 0x55c827ce535b in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:41:29
    #17 0x55c82699a26a in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:857:25
    #18 0x55c8269a2ead in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) content/browser/browser_main_runner_impl.cc:131:15
    #19 0x55c826995caf in content::BrowserMain(content::MainFunctionParams const&) content/browser/browser_main.cc:43:32
    #20 0x55c82a5501c8 in RunBrowserProcessMain content/app/content_main_runner_impl.cc:597:10
    #21 0x55c82a5501c8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:1080:10
    #22 0x55c82a54f1f7 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:955:12
    #23 0x55c82a5482f1 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content/app/content_main.cc:386:36
    #24 0x55c82a5488c7 in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:412:10
    #25 0x55c832671285 in content::BrowserTestBase::SetUp() content/public/test/browser_test_base.cc:698:3
```

```
    #26 0x55c8303a7942 in InProcessBrowserTest::SetUp() chrome/test/base/in_process_browser_test.cc:397:20
    #27 0x55c8213b9d2a in void testing::internal::HandleExceptionsInMethodIfSupported<testing::Test, void>(testing::Test*, void (testing::Test::*)(), char const*)
third_party/googletest/src/googletest/src/gtest.cc
    #28 0x55c8213b97f0 in testing::Test::Run() third_party/googletest/src/googletest/src/gtest.cc:2677:3
    #29 0x55c8213bd035 in testing::TestInfo::Run() third_party/googletest/src/googletest/src/gtest.cc:2861:11
    #30 0x55c8213bf38d in testing::TestSuite::Run() third_party/googletest/src/googletest/src/gtest.cc:3015:28
    #31 0x55c8213fb77d in testing::internal::UnitTestImpl::RunAllTests() third_party/googletest/src/googletest/src/gtest.cc:5855:44
    #32 0x55c8213fa468 in HandleExceptionsInMethodIfSupported<testing::internal::UnitTestImpl, bool> third_party/googletest/src/googletest/src/gtest.cc
    #33 0x55c8213fa468 in testing::UnitTest::Run() third_party/googletest/src/googletest/src/gtest.cc:5438:10
    #34 0x55c83081414f in RUN_ALL_TESTS third_party/googletest/src/googletest/include/gtest/gtest.h:2490:46
    #35 0x55c83081414f in base::TestSuite::Run() base/test/test_suite.cc:462:16
    #36 0x55c830307c6d in RunTestSuiteInternal chrome/test/base/chrome_test_launcher.cc:88:22
    #37 0x55c830307c6d in ChromeTestSuiteRunner::RunTestSuite(int, char**) chrome/test/base/chrome_test_launcher.cc:93:10
    #38 0x55c830307e3d in ChromeTestLauncherDelegate::RunTestSuite(int, char**) chrome/test/base/chrome_test_launcher.cc:134:19
    #39 0x55c832793e36 in content::LaunchTests(content::TestLauncherDelegate*, unsigned long, int, char**) content/public/test/test_launcher.cc:396:31
    #40 0x55c830308574 in LaunchChromeTests(unsigned long, content::TestLauncherDelegate*, int, char**) chrome/test/base/chrome_test_launcher.cc:281:10
    #41 0x55c8302f925f in main chrome/test/base/browser_tests_main.cc:57:10
    #42 0x7f31b996abf6 in __libc_start_main /build/glibc-S7xCS9/glibc-2.27/csu/../csu/libc-start.c:310

0x61e0000a7480 is located 0 bytes inside of 2736-byte region [0x61e0000a7480,0x61e0000a7f30)
freed by thread T0 (browser_tests) here:
    #0 0x55c81999175d in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x55c827daa530 in content::WebContentsImpl::~WebContentsImpl() content/browser/web_contents/web_contents_impl.cc:952:37
    #2 0x55c83d375f03 in operator() buildtools/third_party/libc++/trunk/include/memory:1335:5
    #3 0x55c83d375f03 in reset buildtools/third_party/libc++/trunk/include/memory:1596:7
    #4 0x55c83d375f03 in TabStripModel::SendDetachWebContentsNotifications(TabStripModel::DetachNotifications*) chrome/browser/ui/tabs/tab_strip_model.cc:550:21
    #5 0x55c83d37f506 in TabStripModel::InternalCloseTabs(base::span<content::WebContents* const, 18446744073709551615ul>, unsigned int)
chrome/browser/ui/tabs/tab_strip_model.cc:1816:5
    #6 0x55c83d38082a in TabStripModel::CloseWebContentsAt(int, unsigned int) chrome/browser/ui/tabs/tab_strip_model.cc:760:10
    #7 0x55c83d2283cf in chrome::CloseWebContents(Browser*, content::WebContents*, bool) chrome/browser/ui/browser_tabstrip.cc:91:31
    #8 0x55c83d1cfb02 in CloseContents chrome/browser/ui/browser.cc:1693:5
    #9 0x55c83d1cfb02 in non-virtual thunk to Browser::CloseContents(content::WebContents*) chrome/browser/ui/browser.cc
    #10 0x55c827e48a84 in content::WebContentsImpl::Close(content::RenderViewHost*) content/browser/web_contents/web_contents_impl.cc:7107:16
    #11 0x55c827e04851 in content::WebContentsImpl::Close() content/browser/web_contents/web_contents_impl.cc:4901:3
    #12 0x55c81cc6052f in ChromePageInfoDelegateTest_OpenConnectionHelpCenterPageAfterWebContentsClosed_Test::RunTestOnMainThread()
chrome/browser/ui/page_info/chrome_page_info_delegate_browser_test.cc:87:57
    #13 0x55c83267374c in content::BrowserTestBase::ProxyRunTestOnMainThreadLoop() content/public/test/browser_test_base.cc:849:7
    #14 0x55c832677304 in Invoke<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:509:12
    #15 0x55c832677304 in MakeItSo<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:648:12
    #16 0x55c832677304 in RunImpl<void (content::BrowserTestBase::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserTestBase> >, 0UL>
base/bind_internal.h:721:12
    #17 0x55c832677304 in base::internal::Invoker<base::internal::BindState<void (content::BrowserTestBase::*)(),
base::internal::UnretainedWrapper<content::BrowserTestBase> >, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #18 0x55c830953dac in Run base/callback.h:98:12
    #19 0x55c830953dac in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome/browser/chrome_browser_main.cc:1733:38
    #20 0x55c8309514b5 in ChromeBrowserMainParts::PreMainMessageLoopRun() chrome/browser/chrome_browser_main.cc:1064:18
    #21 0x55c82699ae20 in content::BrowserMainLoop::PreMainMessageLoopRun() content/browser/browser_main_loop.cc:949:28
    #22 0x55c8269a1174 in Invoke<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:509:12
    #23 0x55c8269a1174 in MakeItSo<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:648:12
    #24 0x55c8269a1174 in RunImpl<int (content::BrowserMainLoop::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserMainLoop> >, 0UL>
base/bind_internal.h:721:12
    #25 0x55c8269a1174 in base::internal::Invoker<base::internal::BindState<int (content::BrowserMainLoop::*)(),
base::internal::UnretainedWrapper<content::BrowserMainLoop> >, int ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #26 0x55c827ce535b in Run base/callback.h:98:12
    #27 0x55c827ce535b in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:41:29
    #28 0x55c82699a26a in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:857:25
    #29 0x55c8269a2ead in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) content/browser/browser_main_runner_impl.cc:131:15
    #30 0x55c826995caf in content::BrowserMain(content::MainFunctionParams const&) content/browser/browser_main.cc:43:32
    #31 0x55c82a5501c8 in RunBrowserProcessMain content/app/content_main_runner_impl.cc:597:10
    #32 0x55c82a5501c8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:1080:10
    #33 0x55c82a54f1f7 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:955:12
    #34 0x55c82a5482f1 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content/app/content_main.cc:386:36
    #35 0x55c82a5488c7 in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:412:10
    #36 0x55c832671285 in content::BrowserTestBase::SetUp() content/public/test/browser_test_base.cc:698:3
    #37 0x55c8303a7942 in InProcessBrowserTest::SetUp() chrome/test/base/in_process_browser_test.cc:397:20
    #38 0x55c8213b9d2a in void testing::internal::HandleExceptionsInMethodIfSupported<testing::Test, void>(testing::Test*, void (testing::Test::*)(), char const*)
third_party/googletest/src/googletest/src/gtest.cc
    #39 0x55c8213b97f0 in testing::Test::Run() third_party/googletest/src/googletest/src/gtest.cc:2677:3
    #40 0x55c8213bd035 in testing::TestInfo::Run() third_party/googletest/src/googletest/src/gtest.cc:2861:11
    #41 0x55c8213bf38d in testing::TestSuite::Run() third_party/googletest/src/googletest/src/gtest.cc:3015:28

previously allocated by thread T0 (browser_tests) here:
    #0 0x55c819990efd in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x55c827d9e64d in content::WebContentsImpl::CreateWithOpener(content::WebContents::CreateParams const&, content::RenderFrameHostImpl*)
content/browser/web_contents/web_contents_impl.cc:1061:7
    #2 0x55c827d9e444 in Create content/browser/web_contents/web_contents_impl.cc:562:10
    #3 0x55c827d9e444 in content::WebContents::Create(content::WebContents::CreateParams const&) content/browser/web_contents/web_contents_impl.cc:557:10
    #4 0x55c83d21b4cc in CreateTargetContents chrome/browser/ui/browser_navigator.cc:457:7
    #5 0x55c83d21b4cc in Navigate(NavigateParams*) chrome/browser/ui/browser_navigator.cc:644:28
    #6 0x55c8303a8868 in AddTabAtIndexToBrowser chrome/test/base/in_process_browser_test.cc:492:3
    #7 0x55c8303a8868 in InProcessBrowserTest::AddTabAtIndex(int, GURL const&, ui::PageTransition) chrome/test/base/in_process_browser_test.cc:505:3
    #8 0x55c81cc60415 in ChromePageInfoDelegateTest_OpenConnectionHelpCenterPageAfterWebContentsClosed_Test::RunTestOnMainThread()
chrome/browser/ui/page_info/chrome_page_info_delegate_browser_test.cc:84:3
    #9 0x55c83267374c in content::BrowserTestBase::ProxyRunTestOnMainThreadLoop() content/public/test/browser_test_base.cc:849:7
    #10 0x55c832677304 in Invoke<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:509:12
    #11 0x55c832677304 in MakeItSo<void (content::BrowserTestBase::*)(), content::BrowserTestBase *> base/bind_internal.h:648:12
    #12 0x55c832677304 in RunImpl<void (content::BrowserTestBase::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserTestBase> >, 0UL>
base/bind_internal.h:721:12
    #13 0x55c832677304 in base::internal::Invoker<base::internal::BindState<void (content::BrowserTestBase::*)(),
base::internal::UnretainedWrapper<content::BrowserTestBase> >, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #14 0x55c830953dac in Run base/callback.h:98:12
    #15 0x55c830953dac in ChromeBrowserMainParts::PreMainMessageLoopRunImpl() chrome/browser/chrome_browser_main.cc:1733:38
    #16 0x55c8309514b5 in ChromeBrowserMainParts::PreMainMessageLoopRun() chrome/browser/chrome_browser_main.cc:1064:18
    #17 0x55c82699ae20 in content::BrowserMainLoop::PreMainMessageLoopRun() content/browser/browser_main_loop.cc:949:28
    #18 0x55c8269a1174 in Invoke<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:509:12
    #19 0x55c8269a1174 in MakeItSo<int (content::BrowserMainLoop::*)(), content::BrowserMainLoop *> base/bind_internal.h:648:12
    #20 0x55c8269a1174 in RunImpl<int (content::BrowserMainLoop::*)(), std::tuple<base::internal::UnretainedWrapper<content::BrowserMainLoop> >, 0UL>
base/bind_internal.h:721:12
    #21 0x55c8269a1174 in base::internal::Invoker<base::internal::BindState<int (content::BrowserMainLoop::*)(),
base::internal::UnretainedWrapper<content::BrowserMainLoop> >, int ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:690:12
    #22 0x55c827ce535b in Run base/callback.h:98:12
    #23 0x55c827ce535b in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:41:29
    #24 0x55c82699a26a in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:857:25
```

```
    #25 0x55c8269a2ead in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) content/browser/browser_main_runner_impl.cc:131:15
    #26 0x55c826995caf in content::BrowserMain(content::MainFunctionParams const&) content/browser/browser_main.cc:43:32
    #27 0x55c82a5501c8 in RunBrowserProcessMain content/app/content_main_runner_impl.cc:597:10
    #28 0x55c82a5501c8 in content::ContentMainRunnerImpl::RunBrowser(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:1080:10
    #29 0x55c82a54f1f7 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:955:12
    #30 0x55c82a5482f1 in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) content/app/content_main.cc:386:36
    #31 0x55c82a5488c7 in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:412:10
    #32 0x55c832671285 in content::BrowserTestBase::SetUp() content/public/test/browser_test_base.cc:698:3
    #33 0x55c8303a7942 in InProcessBrowserTest::SetUp() chrome/test/base/in_process_browser_test.cc:397:20
    #34 0x55c8213b9d2a in void testing::internal::HandleExceptionsInMethodIfSupported<testing::Test, void>(testing::Test*, void (testing::Test::*)(), char const*)
third_party/googletest/src/googletest/src/gtest.cc
    #35 0x55c8213b97f0 in testing::Test::Run() third_party/googletest/src/googletest/src/gtest.cc:2677:3
    #36 0x55c8213bd035 in testing::TestInfo::Run() third_party/googletest/src/googletest/src/gtest.cc:2861:11
    #37 0x55c8213bf38d in testing::TestSuite::Run() third_party/googletest/src/googletest/src/gtest.cc:3015:28
    #38 0x55c8213fb77d in testing::internal::UnitTestImpl::RunAllTests() third_party/googletest/src/googletest/src/gtest.cc:5855:44
    #39 0x55c8213fa468 in HandleExceptionsInMethodIfSupported<testing::internal::UnitTestImpl, bool> third_party/googletest/src/googletest/src/gtest.cc
    #40 0x55c8213fa468 in testing::UnitTest::Run() third_party/googletest/src/googletest/src/gtest.cc:5438:10
    #41 0x55c83081414f in RUN_ALL_TESTS third_party/googletest/src/googletest/include/gtest/gtest.h:2490:46
    #42 0x55c83081414f in base::TestSuite::Run() base/test/test_suite.cc:462:16
    #43 0x55c830307c6d in RunTestSuiteInternal chrome/test/base/chrome_test_launcher.cc:88:22
    #44 0x55c830307c6d in ChromeTestSuiteRunner::RunTestSuite(int, char**) chrome/test/base/chrome_test_launcher.cc:93:10

SUMMARY: AddressSanitizer: heap-use-after-free chrome/browser/ui/page_info/chrome_page_info_delegate.cc:177:18 in
ChromePageInfoDelegate::OpenConnectionHelpCenterPage(ui::Event const&)
Shadow bytes around the buggy address:
  0x0c3c8000ce40: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000ce50: fd fd fd fd fd fd fd fd fd fd fa fa fa fa fa fa
  0x0c3c8000ce60: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c8000ce70: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3c8000ce80: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
=>0x0c3c8000ce90:[fd]fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000cea0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000ceb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000cec0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000ced0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3c8000cee0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
Shadow byte legend (one shadow byte represents 8 application bytes):
  Addressable:           00
  Partially addressable: 01 02 03 04 05 06 07
  Heap left redzone:       fa
  Freed heap region:       fd
  Stack left redzone:      f1
  Stack mid redzone:       f2
  Stack right redzone:     f3
  Stack after return:      f5
  Stack use after scope:   f8
  Global redzone:          f9
  Global init order:       f6
  Poisoned by user:        f7
  Container overflow:      fc
  Array cookie:            ac
  Intra object redzone:    bb
  ASan internal:           fe
  Left alloca redzone:     ca
  Right alloca redzone:    cb
  Shadow gap:              cc
==30315==ABORTING
[1/1] ChromePageInfoDelegateTest.OpenConnectionHelpCenterPageAfterWebContentsClosed (CRASHED)
1 test crashed:
    ChromePageInfoDelegateTest.OpenConnectionHelpCenterPageAfterWebContentsClosed
(../../chrome/browser/ui/page_info/chrome_page_info_delegate_browser_test.cc:81)
```

What is the expected behavior?

What went wrong?
when the web_contents_ want to open url, but we can close
the web_contents_ before we use it.

Did this work before? N/A

Chrome version: 91.0.4472.101 Channel: stable
OS Version: 10.0
Flash Version:

chrome_page_info_delegate_browser_test.cc
4.3 KB View Download

Comment 1 by wxhu...@gmail.com on Thu, Jun 10, 2021, 12:48 PM EDT

the patch should like the bug https://bugs.chromium.org/p/chromium/issues/detail?id=1212498. Add the WebContentObserver.

Comment 2 by sheriffbot on Thu, Jun 10, 2021, 12:51 PM EDT Project Member

Labels: external_security_report

Comment 3 by mpdenton@chromium.org on Fri, Jun 11, 2021, 6:25 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: na...@chromium.org
Cc: a...@chromium.org engedy@chromium.org
Labels: Security_Severity-High FoundIn-91
Components: UI>Browser>Bubbles>PageInfo

Thanks for including the browser test and the suggested patch!

nator@ based on https://chromium-review.googlesource.com/c/chromium/src/+/2089710 you might be a good person to look at this bug?

Comment 4 by sheriffbot on Fri, Jun 11, 2021, 6:25 PM EDT Project Member

Labels: Security_Impact-Stable

Comment 5 by sheriffbot on Sat, Jun 12, 2021, 12:47 PM EDT Project Member

Labels: M-91 Target-91

Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 6 by sheriffbot on Sat, Jun 12, 2021, 1:27 PM EDT 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 7 by engedy@chromium.org on Sat, Jun 12, 2021, 7:53 PM EDT Project Member

Cc: olesiamarukhno@google.com dullweber@chromium.org

CC'ing Olesia and Christian who have done a lot of work around Page Info recently. Would either of you have some time to patch this up?

Comment 8 by na...@chromium.org on Fri, Jun 18, 2021, 9:57 AM EDT Project Member

Status: Started (was: Assigned)

Comment 9 by rsesek@chromium.org on Thu, Jul 8, 2021, 5:32 PM EDT Project Member

nator: Have you been able to make progress on this?

Comment 10 by Git Watcher on Fri, Jul 9, 2021, 5:40 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1079ace4a2f90b600e639a64c692922cac3d03da

commit 1079ace4a2f90b600e639a64c692922cac3d03da
Author: Mugdha Lakhani <nator@chromium.org>
Date: Fri Jul 09 09:39:02 2021

[PageInfo] PageInfo UI handles WebContents being destroyed.

A lot of PageInfo and PageInfoUI overrides keep a pointer to
WebContents, which can lead to use after free if WebContents is
destroyed.

The UI should be closed when this happens.

~~Bug: 1218468~~
Change-Id: I9623aab6d1f304fbb629fd8e2880542925ca2aa9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2972872
Commit-Queue: Mugdha Lakhani <nator@chromium.org>
Reviewed-by: Mustafa Emre Acer <meacer@chromium.org>
Reviewed-by: Christian Dullweber <dullweber@chromium.org>
Cr-Commit-Position: refs/heads/master@{#899930}

[modify] https://crrev.com/1079ace4a2f90b600e639a64c692922cac3d03da/chrome/browser/ui/views/page_info/page_info_bubble_view.cc
[modify] https://crrev.com/1079ace4a2f90b600e639a64c692922cac3d03da/chrome/browser/ui/views/page_info/page_info_bubble_view_base.cc
[modify] https://crrev.com/1079ace4a2f90b600e639a64c692922cac3d03da/chrome/browser/ui/views/page_info/page_info_bubble_view_base.h
[modify] https://crrev.com/1079ace4a2f90b600e639a64c692922cac3d03da/chrome/browser/ui/views/page_info/page_info_bubble_view_browsertest.cc
[modify] https://crrev.com/1079ace4a2f90b600e639a64c692922cac3d03da/chrome/browser/ui/views/page_info/page_info_new_bubble_view.cc

Comment 11 by na...@chromium.org on Fri, Jul 16, 2021, 5:19 PM EDT Project Member

Status: Fixed (was: Started)

rsesek@, forgot to mark this as fixed, doing so now.

Comment 12 by sheriffbot on Sat, Jul 17, 2021, 9:06 AM EDT Project Member

Labels: reward-topanel

Comment 13 by sheriffbot on Sat, Jul 17, 2021, 9:10 AM EDT Project Member

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

Comment 14 by sheriffbot on Sat, Jul 17, 2021, 9:10 AM EDT Project Member

Labels: Merge-Request-92 Merge-na Merge-Request-91

Requesting merge to stable M91 because latest trunk commit (899930) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (899930) appears to be after beta branch point (885287).

Not requesting merge to future beta (M93) because latest trunk commit (899930) appears to be prior to future beta branch point (902210). If this is incorrect, please replace the Merge-na label with Merge-Request-93. If other changes are required to fix this bug completely, please request a merge if necessary.

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

Comment 15 by sheriffbot on Sat, Jul 17, 2021, 9:13 AM EDT Project Member

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

This bug requires manual review: We are only 2 days from stable.
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/main/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

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

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

Comment 16 by na...@chromium.org on Mon, Jul 19, 2021, 5:44 AM EDT Project Member

1. Does your merge fit within the Merge Decision Guidelines?
Yes

2. Links to the CLs you are requesting to merge.
https://chromium.googlesource.com/chromium/src/+/1079ace4a2f90b600e639a64c692922cac3d03da

3. Has the change landed and been verified on ToT?
Yes

4. Does this change need to be merged into other active release branches (M-1, M+1)?
M-1

5. Why are these changes required in this milestone after branch?
Externally reported security bug

6. Is this a new feature?
No

7. If it is a new feature, is it behind a flag using finch?
N/A

Comment 17 by na...@chromium.org on Thu, Jul 22, 2021, 11:45 AM EDT Project Member

Cc: benmason@chromium.org
Labels: -Merge-Request-91

Ccing Ben since he said he'll take a look.
Removing merge-Request-91 since M92 stable is out, per guidance from rsesek@.

Comment 18 by amyressler@google.com on Thu, Jul 22, 2021, 4:55 PM EDT Project Member

Labels: reward-0

Apologies, the VRP Panel declines to reward this report as there was exploitability of this issue demonstrated in this report. If you can present how this issues can be exploited by an attacker, either through analysis, a POC, or exploit, we will happy revisit this report and reconsider it for a prospective VRP reward.

We will keep this marked as a security bug for now to provide the time and opportunity to follow up with this information. Thank you!

Comment 19 by wxhu...@gmail.com on Fri, Jul 23, 2021, 4:05 AM EDT

Sorry, I am not familiar with exploit development. hope to see you in next bug.

Comment 20 by amyressler@google.com on Fri, Jul 23, 2021, 12:46 PM EDT Project Member

Labels: Merge-Approved-92 Merge-Approved-91

Merge approved for M-92, please merge to branch 4515 at your earliest convenience.
Also, approving merge to M-91, please do merge to M-91 as this will become the Extended Stable release as we move toward the 4W release cycle. So please also merge to branch 4472. Thanks!

Comment 21 by amyressler@google.com on Fri, Jul 23, 2021, 12:47 PM EDT Project Member

Labels: -Merge-Review-92

Comment 22 by Git Watcher on Mon, Jul 26, 2021, 8:08 AM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b316d13bcc94ebf775a9196cea6832844c6266d2

commit b316d13bcc94ebf775a9196cea6832844c6266d2
Author: Mugdha Lakhani <nator@chromium.org>
Date: Mon Jul 26 12:07:22 2021

[PageInfo] PageInfo UI handles WebContents being destroyed.

A lot of PageInfo and PageInfoUI overrides keep a pointer to
WebContents, which can lead to use after free if WebContents is
destroyed.

The UI should be closed when this happens.

(cherry picked from commit 1079ace4a2f90b600e639a64c692922cac3d03da)

~~Bug: 1218468~~
Change-Id: I9623aab6d1f304fbb629fd8e2880542925ca2aa9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2972872
Commit-Queue: Mugdha Lakhani <nator@chromium.org>
Reviewed-by: Mustafa Emre Acer <meacer@chromium.org>
Reviewed-by: Christian Dullweber <dullweber@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#899930}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3052596
Auto-Submit: Mugdha Lakhani <nator@chromium.org>
Commit-Queue: Mustafa Emre Acer <meacer@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#1578}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/b316d13bcc94ebf775a9196cea6832844c6266d2/chrome/browser/ui/views/page_info/page_info_bubble_view.cc
[modify] https://crrev.com/b316d13bcc94ebf775a9196cea6832844c6266d2/chrome/browser/ui/views/page_info/page_info_bubble_view_base.cc
[modify] https://crrev.com/b316d13bcc94ebf775a9196cea6832844c6266d2/chrome/browser/ui/views/page_info/page_info_bubble_view_base.h
[modify] https://crrev.com/b316d13bcc94ebf775a9196cea6832844c6266d2/chrome/browser/ui/views/page_info/page_info_bubble_view_browsertest.cc
[modify] https://crrev.com/b316d13bcc94ebf775a9196cea6832844c6266d2/chrome/browser/ui/views/page_info/page_info_new_bubble_view.cc

Comment 23 by Git Watcher on Tue, Jul 27, 2021, 10:11 AM EDT Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/252df1b2c738e7da6dedc3a6749ac70f1008c884

commit 252df1b2c738e7da6dedc3a6749ac70f1008c884
Author: Mugdha Lakhani <nator@chromium.org>
Date: Tue Jul 27 14:10:56 2021

[PageInfo] PageInfo UI handles WebContents being destroyed.

A lot of PageInfo and PageInfoUI overrides keep a pointer to
WebContents, which can lead to use after free if WebContents is
destroyed.

The UI should be closed when this happens.

(cherry picked from commit 1079ace4a2f90b600e639a64c692922cac3d03da)

~~Bug: 1218468~~
Change-Id: I9623aab6d1f304fbb629fd8e2880542925ca2aa9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2972872
Commit-Queue: Mugdha Lakhani <nator@chromium.org>
Reviewed-by: Mustafa Emre Acer <meacer@chromium.org>
Reviewed-by: Christian Dullweber <dullweber@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#899930}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3053356
Auto-Submit: Mugdha Lakhani <nator@chromium.org>
Reviewed-by: Balazs Engedy <engedy@chromium.org>
Commit-Queue: Balazs Engedy <engedy@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#1835}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/252df1b2c738e7da6dedc3a6749ac70f1008c884/chrome/browser/ui/views/page_info/page_info_bubble_view.cc
[modify] https://crrev.com/252df1b2c738e7da6dedc3a6749ac70f1008c884/chrome/browser/ui/views/page_info/page_info_bubble_view_base.cc
[modify] https://crrev.com/252df1b2c738e7da6dedc3a6749ac70f1008c884/chrome/browser/ui/views/page_info/page_info_bubble_view_base.h
[modify] https://crrev.com/252df1b2c738e7da6dedc3a6749ac70f1008c884/chrome/browser/ui/views/page_info/page_info_bubble_view_browsertest.cc
[modify] https://crrev.com/252df1b2c738e7da6dedc3a6749ac70f1008c884/chrome/browser/ui/views/page_info/page_info_new_bubble_view.cc

Comment 24 by amyressler@google.com on Wed, Jul 28, 2021, 10:52 AM EDT Project Member
Labels: -reward-topanel

Comment 25 by amyressler@chromium.org on Mon, Aug 2, 2021, 10:33 AM EDT Project Member
Labels: Release-1-M92

Comment 26 by amyressler@google.com on Mon, Aug 2, 2021, 10:57 AM EDT Project Member
Labels: CVE-2021-30594 CVE_description-missing

Comment 27 by voit@google.com on Thu, Aug 5, 2021, 2:28 AM EDT Project Member
Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 28 by gianluca@google.com on Thu, Aug 5, 2021, 6:22 AM EDT Project Member
Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 29 by Git Watcher on Tue, Aug 10, 2021, 2:32 AM EDT Project Member
Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a9eab50a4301957424a651ae15dff7ed0f058535

commit a9eab50a4301957424a651ae15dff7ed0f058535
Author: Zakhar Voit <voit@google.com>
Date: Tue Aug 10 06:31:06 2021

[M90-LTS] [PageInfo] PageInfo UI handles WebContents being destroyed.

A lot of PageInfo and PageInfoUI overrides keep a pointer to
WebContents, which can lead to use after free if WebContents is
destroyed.

The UI should be closed when this happens.

(cherry picked from commit 1079ace4a2f90b600e639a64c692922cac3d03da)

~~Bug: 1218468~~
Change-Id: I9623aab6d1f304fbb629fd8e2880542925ca2aa9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2972872
Commit-Queue: Mugdha Lakhani <nator@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#899930}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3071366
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Zakhar Voit <voit@google.com>
Owners-Override: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1563}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/a9eab50a4301957424a651ae15dff7ed0f058535/chrome/browser/ui/views/page_info/page_info_bubble_view.cc
[modify] https://crrev.com/a9eab50a4301957424a651ae15dff7ed0f058535/chrome/browser/ui/views/page_info/page_info_bubble_view_base.cc
[modify] https://crrev.com/a9eab50a4301957424a651ae15dff7ed0f058535/chrome/browser/ui/views/page_info/page_info_bubble_view_base.h
[modify] https://crrev.com/a9eab50a4301957424a651ae15dff7ed0f058535/chrome/browser/ui/views/page_info/page_info_bubble_view_browsertest.cc

Comment 30 by voit@google.com on Thu, Aug 12, 2021, 3:06 AM EDT Project Member
Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 31 by na...@chromium.org on Mon, Aug 16, 2021, 2:45 PM EDT Project Member
Cc: sporeba@google.com

Comment 32 by amyressler@google.com on Thu, Aug 26, 2021, 1:09 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 33 by sheriffbot on Sun, Oct 24, 2021, 1:29 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