Starred by 8 users

Owner: fergal@chromium.org

CC: hbolaria@chromium.org
rakina@chromium.org
rzanoni@google.com
fergal@chromium.org
kouhei@chromium.org
nhiroki@chromium.org
creis@chromium.org
dcheng@chromium.org
alex...@chromium.org
amyressler@chromium.org
nasko@chromium.org
bfcache-bugs+bug@chromium.org
preloading-bugs@chromium.org
wfh@chromium.org
altimin@chromium.org
ajgo@chromium.org

Status: Fixed *(Closed)*

Components: Internals>Sandbox>SiteIsolation
UI>Browser>Navigation>BFCache
Internals>Preload>Prerender

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
reward-decline
Arch-x86_64
Deadline-Exceeded
Security_Severity-High
allpublic
Via-Wizard-Security
CVE_description-submitted
external_security_report

M-98
Target-96
Target-98

Issue 1283050: Heap-use-after-free in RenderViewHostImpl::ActivatePrerenderedPage

Reported by samet...@gmail.com on Tue, Dec 28, 2021, 10:22 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36

Steps to reproduce the problem:
PoC:

click

1) Click the link.
2) Enter google.com in the search bar and go.
3) Click to go back and wait for the page to load.
4) Click to go back.
5) Uaf.

What is the expected behavior?

What went wrong?
==========
==8092==ERROR: AddressSanitizer: heap-use-after-free on address 0x1218327e5cd0 at pc 0x7ffaca918f62 bp 0x0015651fdd20 sp 0x0015651fdd68
READ of size 8 at 0x1218327e5cd0 thread T0
==8092==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ffaca918f61 in content::RenderViewHostImpl::ActivatePrerenderedPage C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_view_host_impl.cc:575
    #1 0x7ffaca7e0bf5 in content::PageImpl::ActivateForPrerendering C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\page_impl.cc:174
    #2 0x7ffaca8a06bf in content::RenderFrameHostManager::CommitPending C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:3331
    #3 0x7ffaca89f5f0 in content::RenderFrameHostManager::CommitPendingIfNecessary C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:488
    #4 0x7ffaca89f2a6 in content::RenderFrameHostManager::DidNavigateFrame C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:457
    #5 0x7ffaca7cff34 in content::Navigator::DidNavigate C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigator.cc:467
    #6 0x7ffaca819a0b in content::RenderFrameHostImpl::DidCommitNavigationInternal C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc:10600
    #7 0x7ffaca817687 in content::RenderFrameHostImpl::DidCommitNavigation C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc:11127
    #8 0x7ffaca8982b4 in base::internal::Invoker<base::internal::BindState<void (content::RenderFrameHostImpl::*)(content::NavigationRequest *, mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>, mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>),base::internal::UnretainedWrapper<content::RenderFrameHostImpl>,base::internal::UnretainedWrapper<content::NavigationRequest> >,void (mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>, mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>)>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:741
    #9 0x7ffac9020327 in base::OnceCallback<void (mojo::StructPtr<content::mojom::DidCommitProvisionalLoadParams>,

mojo::StructPtr<content::mojom::DidCommitProvisionalLoadInterfaceParams>)>::Run
C:\b\s\w\ir\cache\builder\src\base\callback.h:142
    #10 0x7ffac9020d7d in content::mojom::NavigationClient_CommitFailedNavigation_ForwardToCallback::Accept
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\content\common\navigation_client.mojom.cc:1122
    #11 0x7ffad0eed50d in mojo::InterfaceEndpointClient::HandleValidatedMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:895
    #12 0x7ffad38219f2 in mojo::MessageDispatcher::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #13 0x7ffad0ef0ea4 in mojo::InterfaceEndpointClient::HandleIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:657
    #14 0x7ffad177f7db in IPC::`anonymous namespace'::ChannelAssociatedGroupController::AcceptOnEndpointThread
C:\b\s\w\ir\cache\builder\src\ipc\ipc_mojo_bootstrap.cc:1008
    #15 0x7ffad17793f7 in base::internal::Invoker<base::internal::BindState<void (IPC::(anonymous
namespace)::ChannelAssociatedGroupController::*)(mojo::Message),scoped_refptr<IPC::(anonymous
namespace)::ChannelAssociatedGroupController>,mojo::Message>,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:741
    #16 0x7ffad0ba0d04 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
    #17 0x7ffad36daf15 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #18 0x7ffad36da5e8 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #19 0x7ffad0c48b56 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #20 0x7ffad0c46de8 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #21 0x7ffad36dc5e1 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #22 0x7ffad0b1f873 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
    #23 0x7ffac9d3fe41 in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1048
    #24 0x7ffac9d45261 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
    #25 0x7ffac9d394c9 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:30
    #26 0x7ffacc7c9223 in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
    #27 0x7ffacc7cc263 in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1160
    #28 0x7ffacc7cb396 in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1026
    #29 0x7ffacc7c766d in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:398
    #30 0x7ffacc7c86f8 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:426
    #31 0x7ffac608148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:177
    #32 0x7ff62e725b85 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #33 0x7ff62e722b5f in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #34 0x7ff62eb2753f in __scrt_common_main_seh
d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #35 0x7ffb822454df in BaseThreadInitThunk+0xf (C:\WINDOWS\System32\KERNEL32.DLL+0x1800154df)
    #36 0x7ffb833e485a in RtlUserThreadStart+0x2a (C:\WINDOWS\SYSTEM32\ntdll.dll+0x18000485a)

0x1218327e5cd0 is located 592 bytes inside of 624-byte region [0x1218327e5a80,0x1218327e5cf0)
freed by thread T0 here:
    #0 0x7ff62e7d23fb in free C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:82

```
    #1 0x7ffaca91cb5f in content::RenderViewHostImpl::~RenderViewHostImpl
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_view_host_impl.cc:345
    #2 0x7ffaca7f64f5 in content::RenderFrameHostImpl::~RenderFrameHostImpl
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc:1660
    #3 0x7ffaca876eb1 in content::RenderFrameHostImpl::~RenderFrameHostImpl
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc:1514
    #4 0x7ffaca8a4b43 in content::RenderFrameHostManager::DiscardUnusedFrame
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:778
    #5 0x7ffaca89edd5 in content::RenderFrameHostManager::CleanUpNavigation
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:1248
    #6 0x7ffaca807494 in content::RenderFrameHostImpl::RenderProcessExited
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_impl.cc:2858
    #7 0x7ffaca8ed417 in content::RenderProcessHostImpl::ProcessDied
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_process_host_impl.cc:4757
    #8 0x7ffad0ba0d04 in base::TaskAnnotator::RunTaskImpl
C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:135
    #9 0x7ffad36daf15 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:356
    #10 0x7ffad36da5e8 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:261
    #11 0x7ffad0c48b56 in base::MessagePumpForUI::DoRunLoop
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #12 0x7ffad0c46de8 in base::MessagePumpWin::Run
C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #13 0x7ffad36dc5e1 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:468
    #14 0x7ffad0b1f873 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:140
    #15 0x7ffac9d3fe41 in content::BrowserMainLoop::RunMainMessageLoop
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:1048
    #16 0x7ffac9d45261 in content::BrowserMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:153
    #17 0x7ffac9d394c9 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:30
    #18 0x7ffacc7c9223 in content::RunBrowserProcessMain
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:646
    #19 0x7ffacc7cc263 in content::ContentMainRunnerImpl::RunBrowser
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1160
    #20 0x7ffacc7cb396 in content::ContentMainRunnerImpl::Run
C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1026
    #21 0x7ffacc7c766d in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:398
    #22 0x7ffacc7c86f8 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:426
    #23 0x7ffac608148e in ChromeMain C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_main.cc:177
    #24 0x7ff62e725b85 in MainDllLoader::Launch C:\b\s\w\ir\cache\builder\src\chrome\app\main_dll_loader_win.cc:169
    #25 0x7ff62e722b5f in main C:\b\s\w\ir\cache\builder\src\chrome\app\chrome_exe_main_win.cc:382
    #26 0x7ff62eb2753f in __scrt_common_main_seh
d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #27 0x7ffb822454df in BaseThreadInitThunk+0xf (C:\WINDOWS\System32\KERNEL32.DLL+0x1800154df)

previously allocated by thread T0 here:
    #0 0x7ff62e7d24fb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffae3361fbe in operator new d:\A01\_work\6\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffaca9130c4 in content::RenderViewHostFactory::Create
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_view_host_factory.cc:41
    #3 0x7ffaca60127a in content::FrameTree::CreateRenderViewHost
```

C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\frame_tree.cc:642
#4 0x7ffaca8b1c73 in content::RenderFrameHostManager::CreateRenderFrameProxy
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:2831
#5 0x7ffaca5fc895 in content::FrameTree::CreateProxiesForSiteInstance
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\frame_tree.cc:551
#6 0x7ffaca8b0dc0 in content::RenderFrameHostManager::CreateProxiesForNewRenderFrameHost
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:2522
#7 0x7ffaca8a966a in content::RenderFrameHostManager::CreateSpeculativeRenderFrameHost
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:2674
#8 0x7ffaca8a6ff4 in content::RenderFrameHostManager::GetFrameHostForNavigation
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:1085
#9 0x7ffaca78a680 in content::NavigationRequest::OnRequestFailedInternal
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc:3604
#10 0x7ffaca7a87b3 in content::NavigationRequest::OnWillProcessResponseChecksComplete
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc:4201
#11 0x7ffaca7b00a8 in content::NavigationRequest::OnWillProcessResponseProcessed
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc:5346
#12 0x7ffaca7af2e4 in content::NavigationRequest::OnNavigationEventProcessed
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc:5252
#13 0x7ffaca7cc850 in content::NavigationThrottleRunner::ProcessInternal
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_throttle_runner.cc:245
#14 0x7ffaca79dcc9 in content::NavigationRequest::OnResponseStarted
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_request.cc:3452
#15 0x7ffaca38e0a5 in content::NavigationURLLoaderImpl::NotifyResponseStarted
C:\b\s\w\ir\cache\builder\src\content\browser\loader\navigation_url_loader_impl.cc:1467
#16 0x7ffaca398b64 in base::internal::FunctorTraits<void (content::NavigationURLLoaderImpl::*)
(mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>,
mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, const content::GlobalRequestID &, bool),void>::Invoke<void
(content::NavigationURLLoaderImpl::*)(mojo::StructPtr<network::mojom::URLResponseHead>,
mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>,
mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, const content::GlobalRequestID &,
bool),base::WeakPtr<content::NavigationURLLoaderImpl>,mojo::StructPtr<network::mojom::URLResponseHead>,mojo::Stru
ctPtr<network::mojom::URLLoaderClientEndpoints>,mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>,content::
GlobalRequestID,bool> C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:535
#17 0x7ffaca3988eb in base::internal::Invoker<base::internal::BindState<void (content::NavigationURLLoaderImpl::*)
(mojo::StructPtr<network::mojom::URLResponseHead>, mojo::StructPtr<network::mojom::URLLoaderClientEndpoints>,
mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>, const content::GlobalRequestID &,
bool),base::WeakPtr<content::NavigationURLLoaderImpl>,mojo::StructPtr<network::mojom::URLResponseHead>,mojo::Stru
ctPtr<network::mojom::URLLoaderClientEndpoints>,mojo::ScopedHandleBase<mojo::DataPipeConsumerHandle>,content::
GlobalRequestID,bool>,void ()>::RunOnce C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:741
#18 0x7ffaca38e547 in content::NavigationURLLoaderImpl::ParseHeaders
C:\b\s\w\ir\cache\builder\src\content\browser\loader\navigation_url_loader_impl.cc:1145
#19 0x7ffaca38d94a in content::NavigationURLLoaderImpl::CallOnReceivedResponse
C:\b\s\w\ir\cache\builder\src\content\browser\loader\navigation_url_loader_impl.cc:872
#20 0x7ffaca38be9b in content::NavigationURLLoaderImpl::OnStartLoadingResponseBody
C:\b\s\w\ir\cache\builder\src\content\browser\loader\navigation_url_loader_impl.cc:825
#21 0x7ffac8ec7a46 in blink::ThrottlingURLLoader::OnStartLoadingResponseBody
C:\b\s\w\ir\cache\builder\src\third_party\blink\common\loader\throttling_url_loader.cc:836
#22 0x7ffac7d264b9 in network::mojom::URLLoaderClientStubDispatch::Accept
C:\b\s\w\ir\cache\builder\src\out\Release_x64\gen\services\network\public\mojom\url_loader.mojom.cc:1212
#23 0x7ffad0eed699 in mojo::InterfaceEndpointClient::HandleValidatedMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:900
#24 0x7ffad38219f2 in mojo::MessageDispatcher::Accept

```
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43
    #25 0x7ffad0ef0ea4 in mojo::InterfaceEndpointClient::HandleIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:657
    #26 0x7ffad0f04cf5 in mojo::internal::MultiplexRouter::ProcessIncomingMessage
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:1104
    #27 0x7ffad0f03ac7 in mojo::internal::MultiplexRouter::Accept
C:\b\s\w\ir\cache\builder\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:724

SUMMARY: AddressSanitizer: heap-use-after-free
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_view_host_impl.cc:575 in
content::RenderViewHostImpl::ActivatePrerenderedPage
Shadow bytes around the buggy address:
  0x042f38bfcb40: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x042f38bfcb50: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcb60: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcb70: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcb80: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x042f38bfcb90: fd fd fd fd fd fd fd fd fd fd[fd]fd fd fd fa fa
  0x042f38bfcba0: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x042f38bfcbb0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcbc0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcbd0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x042f38bfcbe0: 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
==8092==ABORTING
```

Did this work before? N/A

Chrome version: 96.0.4664.110 Channel: stable
OS Version: 10.0

Thanks,

Samet Bekmezci @sametbekmezci

asan.log

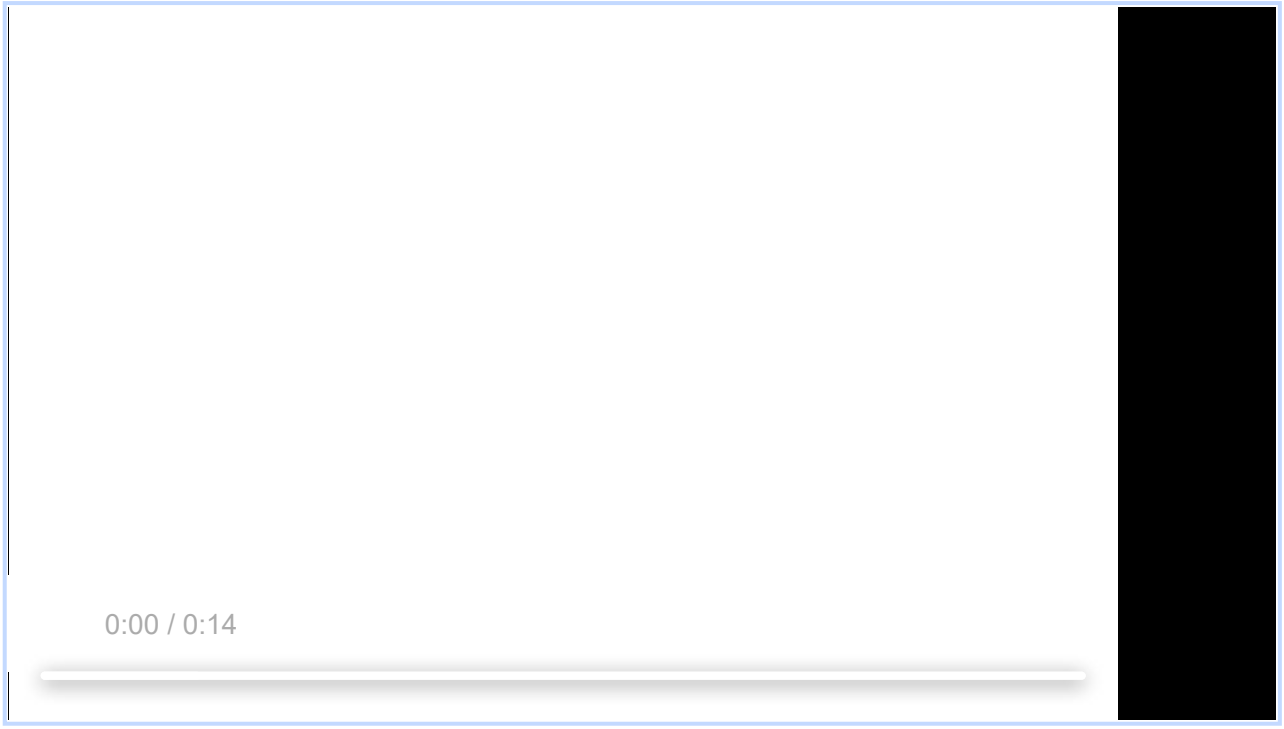
17.6 KB View Download

Comment 1 by sheriffbot on Tue, Dec 28, 2021, 10:23 AM EST Project Member

Labels: external_security_report

Comment 2 by samet...@gmail.com on Tue, Dec 28, 2021, 11:50 AM EST

poc.mp4
1.9 MB View Download



Comment 3 by samet...@gmail.com on Tue, Dec 28, 2021, 5:17 PM EST

I think the problem is with `PageImpl::ActivateForPrerendering`. In the loop `render_view_hosts` is freed and the next step is UaF. [1]

[1] https://source.chromium.org/chromium/chromium/src/+/main:content/browser/renderer_host/page_impl.cc;drc=5c606c1664b0ecfe31dfc6e33993b76a1fca37fa;l=174

Comment 4 by mpdenton@chromium.org on Thu, Dec 30, 2021, 7:20 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: nhiroki@chromium.org
Labels: Security_Severity-High FoundIn-96
Components: UI>Browser>Navigation>BFCache Internals>Preload>Prerender

Comment 5 by mpdenton@chromium.org on Thu, Dec 30, 2021, 7:21 PM EST Project Member

Cc: falken@chromium.org hbolaria@chromium.org

I'm not entirely sure I've triaged this to the right person, so adding some others.

Comment 6 by mpdenton@chromium.org on Thu, Dec 30, 2021, 7:22 PM EST Project Member

Labels: OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Lacros

This also repros reliably for me.

Comment 7 by sheriffbot on Thu, Dec 30, 2021, 7:22 PM EST Project Member

Labels: Security_Impact-Extended

Comment 8 by sheriffbot on Fri, Dec 31, 2021, 12:46 PM EST Project Member

Labels: Target-96 M-96

Setting milestone and target because of high severity.

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

Comment 9 by sheriffbot on Fri, Dec 31, 2021, 1:06 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 10 by creis@chromium.org on Wed, Jan 5, 2022, 1:19 PM EST Project Member

Owner: kouhei@chromium.org
Cc: nhiroki@chromium.org
Labels: OS-Android

kouhei@: It looks like nhiroki@ is OOO for a bit. Can you help find an owner or take a look? Thanks!

Comment 11 by nhiroki@chromium.org on Mon, Jan 10, 2022, 7:24 PM EST Project Member

Owner: nhiroki@chromium.org
Cc: -falken@chromium.org -nhiroki@chromium.org kouhei@chromium.org

I'll take a look.

Comment 12 by nhiroki@chromium.org on Thu, Jan 13, 2022, 10:08 AM EST Project Member

Status: Started (was: Assigned)

Comment 13 by nhiroki@chromium.org on Thu, Jan 13, 2022, 10:23 AM EST Project Member

Hmmm, RenderViewHostImpl seems to be destroyed due to destruction of renderer process hosting the RVHI, but the set of RVHIs doesn't handle the case. We could change the value type of the set from RenderViewHostImpl* to WeakPtr<RenderViewHostImpl> and then check if it's still alive before accessing it. I'll make a patch.

Comment 14 by creis@chromium.org on Thu, Jan 13, 2022, 12:52 PM EST Project Member

Cc: creis@chromium.org dcheng@chromium.org
Components: Internals>Sandbox>SiteIsolation

Comment 13: Thanks! Something sounds unexpected there, or at least phrased in a way I wouldn't expect. Generally RenderViewHostImpl sticks around if the process exits (e.g., sad tab), but then returns false from IsRenderViewLive (due to the change to renderer_view_created_ in RVHI::RenderProcessExited). If the RenderViewHostImpl itself is being deleted,

that's usually in response to not being needed anymore (e.g., after all of its RenderFrameHosts and RenderProxyHosts have gone away after a navigation).

Which set of RVHIs are you referring to here? I think dcheng@ and I might be interested in the fix you're proposing, given some similar work we're doing in ~~issue 1260007~~. Thanks!

Comment 15 by nhiroki@chromium.org on Fri, Jan 14, 2022, 8:51 AM EST Project Member

This crash happens here in PageImpl::ActivateForPrerendering():
https://source.chromium.org/chromium/chromium/src/+/main:content/browser/renderer_host/page_impl.cc;l=174;drc=751bbeb73a0dacc98a2b9486e0cf788fe763356a

This `rvh` is retrieved from `std::set<RenderViewHostImpl*>& render_view_hosts` passed from the caller of PageImpl::ActivateForPrerendering(). This set originally comes from StoredPage::render_view_hosts:
https://source.chromium.org/chromium/chromium/src/+/main:content/browser/renderer_host/stored_page.h;l=52;drc=751bbeb73a0dacc98a2b9486e0cf788fe763356a

I'm not sure about the lifetime model of StoredPage::render_view_hosts. Is it expected to be valid until StoredPage gets destroyed?

Comment 16 by nhiroki@chromium.org on Fri, Jan 14, 2022, 11:39 AM EST Project Member

I tried to reproduce this on my local environment (the current ToT on Linux). In my case, the browser hit the following DCHECK on the step 3. This happens even when Prerender2 is explicitly disabled by chrome://flags.

[2012253:2012253:0115/012240.661693:FATAL:navigation_request.cc(6157)] Check failed: params->url_is_unreachable == false (1 vs. 0)

This is the stacktrace. This seems to happen during the bfcache restore.

Received signal 6
#0 0x7fbb4310df5f base::debug::CollectStackTrace()
#1 0x7fbb42e66c0a base::debug::StackTrace::StackTrace()
#2 0x7fbb42e66bc5 base::debug::StackTrace::StackTrace()
#3 0x7fbb4310da2c base::debug::(anonymous namespace)::StackDumpSignalHandler()
#4 0x7fbb05726200 (/usr/lib/x86_64-linux-gnu/libpthread-2.33.so+0x131ff)
#5 0x7fbb04eb6891 gsignal
#6 0x7fbb04ea0536 abort
#7 0x7fbb4310d286 base::debug::(anonymous namespace)::DebugBreak()
#8 0x7fbb4310d265 base::debug::BreakDebuggerAsyncSafe()
#9 0x7fbb42e62e39 base::debug::BreakDebugger()
#10 0x7fbb42eb5a89 logging::LogMessage::~LogMessage()
#11 0x7fbb42eb5b99 logging::LogMessage::~LogMessage()
#12 0x7fbb42e2085b logging::CheckError::~CheckError()
#13 0x7fbb3b3725f9 content::NavigationRequest::MakeDidCommitProvisionalLoadParamsForActivation()
#14 0x7fbb3b367199 content::NavigationRequest::MakeDidCommitProvisionalLoadParamsForBFCacheRestore()
#15 0x7fbb3b366ee2 content::NavigationRequest::CommitPageActivation()
#16 0x7fbb3b358b93 content::NavigationRequest::CommitNavigation()
#17 0x7fbb3b36570c content::NavigationRequest::OnCommitDeferringConditionChecksComplete()
#18 0x7fbb3b133f4e content::CommitDeferringConditionRunner::ProcessConditions()
#19 0x7fbb3b134148 content::CommitDeferringConditionRunner::ResumeProcessing()
#20 0x7fbb3b1378cf base::internal::FunctorTraits<>::Invoke<>()
#21 0x7fbb3b1377b7 base::internal::InvokeHelper<>::MakeItSo<>()

#22 0x7fbb3b137722
_ZN4base8internal7InvokerINS0_9BindStateIMN7content30CommitDeferringConditionRunnerEFvvEJNS_7WeakPtrIS4_E
EEEEFvvEE7RunImplIS6_NSt4__Cr5tupleIJS8_EEEJLm0EEEEvOT_OT0_NSD_16integer_sequenceImJXspT1_EEEE
#23 0x7fbb3b13765c base::internal::Invoker<>::RunOnce()
#24 0x7fbb390d1541 _ZNO4base12OnceCallbackIFvvEE3RunEv
#25 0x7fbb3b105248 content::BackForwardCacheImpl::WillCommitNavigationToCachedEntry()::$_3::operator()()
#26 0x7fbb3b105207 base::internal::FunctorTraits<>::Invoke<>()
#27 0x7fbb3b1051a7 base::internal::InvokeHelper<>::MakeItSo<>()
#28 0x7fbb3b105143
_ZN4base8internal7InvokerINS0_9BindStateIZN7content20BackForwardCacheImpl33WillCommitNavigationToCachedEntr
yERNS4_5EntryENS_12OnceCallbackIFvvEEEE3$_3JNS_9TimeTicksES9_EEES8_E7RunImplISA_NSt4__Cr5tupleIJSB
_S9_EEEJLm0ELm1EEEEvOT_OT0_NSF_16integer_sequenceImJXspT1_EEEE
#29 0x7fbb3b10504c base::internal::Invoker<>::RunOnce()
#30 0x7fbb42e166a1 _ZNO4base12OnceCallbackIFvvEE3RunEv
#31 0x7fbb42e1ae6d base::(anonymous namespace)::BarrierInfo::Run()
#32 0x7fbb42e1b48f base::internal::FunctorTraits<>::Invoke<>()
#33 0x7fbb42e1b391 base::internal::InvokeHelper<>::MakeItSo<>()
#34 0x7fbb42e1b332
_ZN4base8internal7InvokerINS0_9BindStateIMNS_12_GLOBAL__N_111BarrierInfoEFvvEJNSt4__Cr10unique_ptrIS4_NS
7_14default_deleteIS4_EEEEEEFvvEE7RunImplIRKS6_RKNS7_5tupleIJSB_EEEJLm0EEEEvOT_OT0_NS7_16integer_
sequenceImJXspT1_EEEE
#35 0x7fbb42e1b277 base::internal::Invoker<>::Run()
#36 0x7fbb390d1541 _ZNO4base12OnceCallbackIFvvEE3RunEv
#37 0x7fbb3b3b0412 content::PageLifecycleStateManager::OnPageLifecycleChangedAck()
#38 0x7fbb3b3b1ed1 base::internal::FunctorTraits<>::Invoke<>()
#39 0x7fbb3b3b1d61 base::internal::InvokeHelper<>::MakeItSo<>()
#40 0x7fbb3b3b1ca4
_ZN4base8internal7InvokerINS0_9BindStateIMN7content25PageLifecycleStateManagerEFvN4mojo9StructPtrIN5blink5mo
jom18PageLifecycleStateEEENS_12OnceCallbackIFvvEEEJNS_7WeakPtrIS4_EESA_SD_EEESC_E7RunImplISF_NSt4
__Cr5tupleIJSH_SA_SD_EEEJLm0ELm1ELm2EEEEvOT_OT0_NSL_16integer_sequenceImJXspT1_EEEE
#41 0x7fbb3b3b1b6c base::internal::Invoker<>::RunOnce()
#42 0x7fbb2f375931 _ZNO4base12OnceCallbackIFvvEE3RunEv
#43 0x7fbb2fdc3d2d blink::mojom::PageBroadcast_SetPageLifecycleState_ForwardToCallback::Accept()
#44 0x7fbb41cff2a8 mojo::InterfaceEndpointClient::HandleValidatedMessage()
#45 0x7fbb41cfeb69 mojo::InterfaceEndpointClient::HandleIncomingMessageThunk::Accept()
#46 0x7fbb41d177ab mojo::MessageDispatcher::Accept()
#47 0x7fbb41d00f0f mojo::InterfaceEndpointClient::HandleIncomingMessage()
#48 0x7fbb3f1faf3a IPC::(anonymous namespace)::ChannelAssociatedGroupController::AcceptOnEndpointThread()
#49 0x7fbb3f1efdee base::internal::FunctorTraits<>::Invoke<>()
#50 0x7fbb3f1efc96 base::internal::InvokeHelper<>::MakeItSo<>()
#51 0x7fbb3f1efc03
_ZN4base8internal7InvokerINS0_9BindStateIMN3IPC12_GLOBAL__N_132ChannelAssociatedGroupControllerEFvN4moj
o7MessageEEJ13scoped_refptrIS5_ES7_EEEFvvEE7RunImplIS9_NSt4__Cr5tupleIJSB_S7_EEEJLm0ELm1EEEEvOT_O
T0_NSG_16integer_sequenceImJXspT1_EEEE
#52 0x7fbb3f1efb0c base::internal::Invoker<>::RunOnce()
#53 0x7fbb42e166a1 _ZNO4base12OnceCallbackIFvvEE3RunEv
#54 0x7fbb43000456 base::TaskAnnotator::RunTaskImpl()
#55 0x7fbb43057340 base::TaskAnnotator::RunTask<>()
#56 0x7fbb430570e2 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl()
#57 0x7fbb43056889 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#58 0x7fbb430572c0 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
#59 0x7fbb42edf6b1 base::MessagePumpGlib::Run()
#60 0x7fbb43057842 base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run()

#61 0x7fbb42f908f7 base::RunLoop::Run()
#62 0x7fbb3a5bb31c content::BrowserMainLoop::RunMainMessageLoop()
#63 0x7fbb3a5c8a0f content::BrowserMainRunnerImpl::Run()
#64 0x7fbb3a5b7176 content::BrowserMain()
#65 0x7fbb3c96b089 content::RunBrowserProcessMain()
#66 0x7fbb3c96cccc content::ContentMainRunnerImpl::RunBrowser()
#67 0x7fbb3c96c4ab content::ContentMainRunnerImpl::Run()
#68 0x7fbb3c968e28 content::RunContentProcess()
#69 0x7fbb3c9697aa content::ContentMain()
#70 0x56126438240a ChromeMain
#71 0x561264382232 main
#72 0x7fbb04ea17ed __libc_start_main
#73 0x56126438214a _start
 r8: 0000000000000000 r9: 00007fff15718770 r10: 0000000000000008 r11: 0000000000000246
r12: 0000561264382120 r13: 0000000000000000 r14: 0000000000000000 r15: 0000000000000000
 di: 0000000000000002 si: 00007fff15718770 bp: 00007fff157189c0 bx: 00007fbaf1133540
 dx: 0000000000000000 ax: 0000000000000000 cx: 00007fbb04eb6891 sp: 00007fff15718770
 ip: 00007fbb04eb6891 efl: 0000000000000246 cgf: 002b000000000033 erf: 0000000000000000
trp: 0000000000000000 msk: 0000000000000000 cr2: 0000000000000000
[end of stack trace]

Comment 17 by nhiroki@chromium.org on Fri, Jan 14, 2022, 11:50 AM EST Project Member

Anyone in the BFCache team can take a look at #c16? This could hide or supersede the original issue.

I ran out of time today. I'll investigate behavior on older versions (e.g., stable 96 as reporter used) next time.

Comment 18 by samet...@gmail.com on Fri, Jan 14, 2022, 12:20 PM EST

Hi nhiroki, After pressing the "go back" button for the first time, you must wait for the page to load. If you don't wait and click the "go back" button again, DCHECK will occur. If you wait before pressing the "go back" button again, as in the video I shared above, it will become UaF. #0

Comment 19 by nhiroki@chromium.org on Mon, Jan 17, 2022, 8:09 AM EST Project Member

#c18: Thanks for the follow-up! On my environment, the check failure on #c16 happens during the first "go back" navigation.

I'll file a separate issue for the check failure so that the BFCache team can take a look separately.

Comment 20 by nhiroki@chromium.org on Mon, Jan 17, 2022, 8:22 AM EST Project Member

Blockedon: 1287996

Comment 21 by nhiroki@chromium.org on Mon, Jan 17, 2022, 10:54 AM EST Project Member

I built previous versions and tried to reproduce this:
- 97.0.4692.95 (stable) didn't reproduce.
- 98.0.4758.60 (beta) hit the DCHECK failure on #c16.

Comment 22 by samet...@gmail.com on Mon, Jan 17, 2022, 11:01 AM EST

#c2 My version in the video:
99.0.4784.0 (Developer Build) (64-bit)

OS: Windows 11 Version 21H2 (Build 22000.434)

Comment 23 by nhiroki@chromium.org on Tue, Jan 18, 2022, 5:21 AM EST Project Member

Cc: fergal@chromium.org

cc: fergal@ for visibility.

Comment 24 by sheriffbot on Wed, Feb 2, 2022, 12:21 PM EST Project Member

Labels: -M-96 M-98 Target-98

Comment 25 by samet...@gmail.com on Mon, Feb 14, 2022, 6:39 AM EST

Hi nhiroki@, friendly ping!

this-is-fine.jpg
65.6 KB View Download

Comment 26 by mpdenton@chromium.org on Mon, Feb 21, 2022, 10:29 PM EST Project Member

Hi nhiroki@, friendly security team ping, any update on this bug?

Comment 27 by sheriffbot on Sun, Feb 27, 2022, 1:45 PM EST Project Member

Labels: Deadline-Exceeded

We commit ourselves to a 60 day deadline for fixing for high severity vulnerabilities, and have exceeded it here. If you're unable to look into this soon, could you please find another owner or remove yourself so that this gets back into the security triage queue?

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

Comment 28 by nhiroki@chromium.org on Tue, Mar 8, 2022, 6:05 AM EST Project Member

Sorry for the late reply. I tried to reproduce the issue on the Windows 11 and Linux with the latest developer build again but failed due to the DCHECK failure at #c16. Commenting out the dcheck causes another crash on dereferencing an invalid absl::nullopt in MakeDidCommitProvisionalLoadParamsForBFCacheRestore().

I'm now wondering if some state on BFCache could be broken and it could unexpectedly call PageImpl::ActivateForPrerendering() (see the original crash) in:
https://source.chromium.org/chromium/chromium/src/+/main:content/browser/renderer_host/render_frame_host_manager.cc;l=3385-3405;drc=753cc53862e4d455bd7e1b354d94ceb919f2f4cb

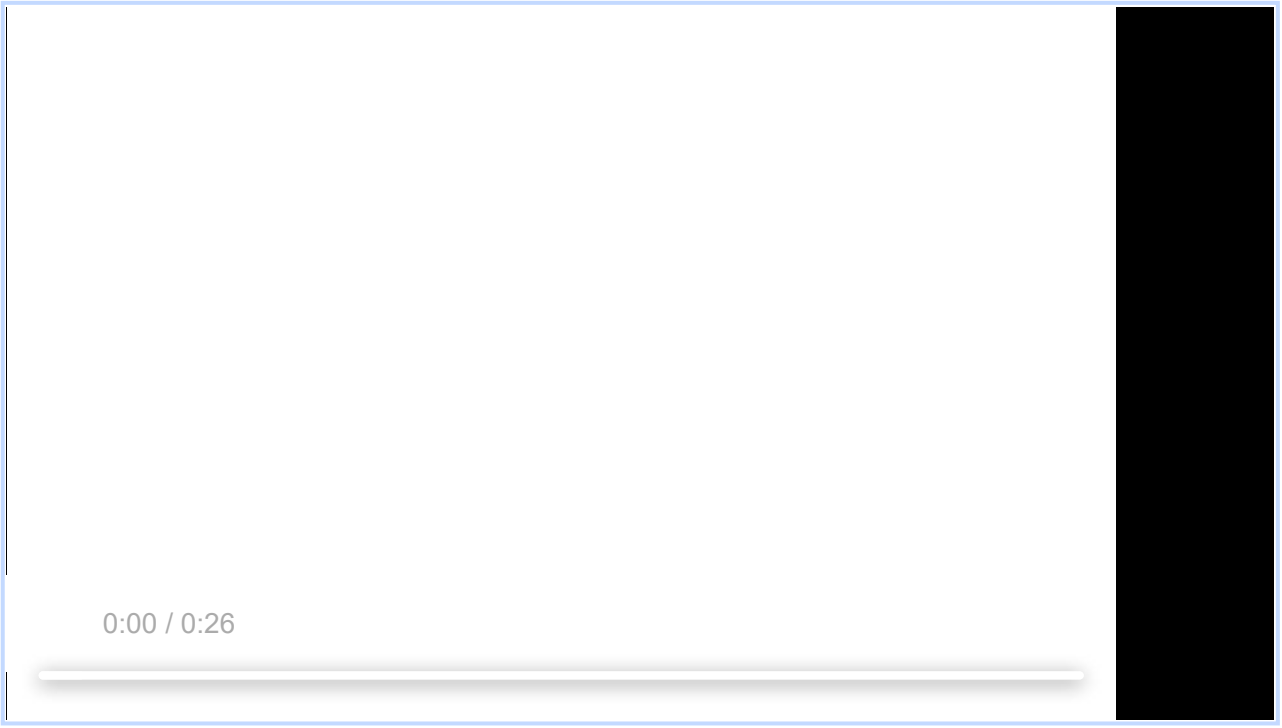
sametforuaf@: Are you still able to reproduce this issue with the latest developer build? Do you enable experimental features on chrome://flags?

Comment 29 by samet...@gmail.com on Tue, Mar 8, 2022, 3:42 PM EST

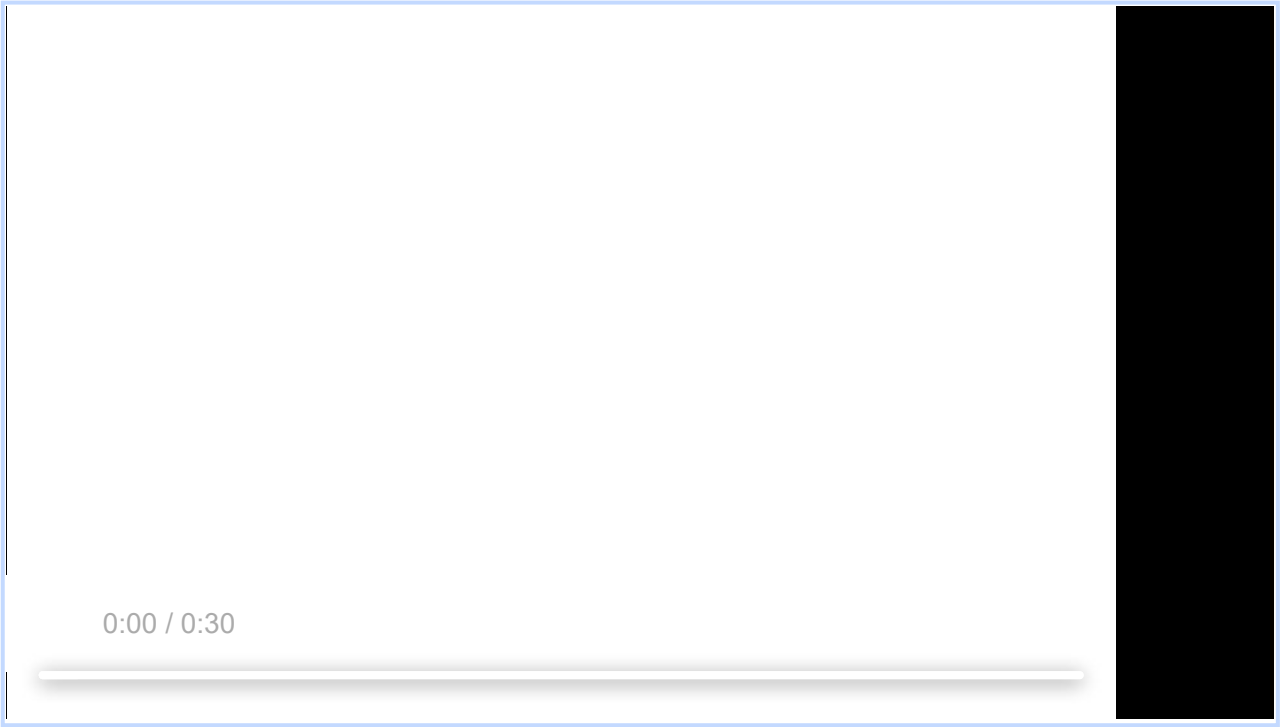
1) I am able to reproduce it in the latest version.
2) No.

Can you share a video with the steps?

poc1.mp4
4.2 MB View Download



poc2.mp4
4.5 MB View Download



Comment 30 by nhiroki@chromium.org on Wed, Mar 9, 2022, 9:54 AM EST Project Member

Cc: rakina@chromium.org

#c29: Thanks! Sorry, I didn't have time to take a video today. I'll do it next time.

By the way, I'm wondering if this issue could be caused by BFCache, not Prerender2. Prerender2 is still behind a feature flag and the reporter doesn't explicitly enable it on chrome://flags. The feature could implicitly be enabled by some field trials but it shouldn't be applicable to developer builds. Also, on poc1.mp4, there is no chance to run Prerender2 (it doesn't work for chrome://version and a warning page), but BFCache could run for them.

Based on the above, I'd like to put this issue on hold until ~~issue 1287996~~ gets resolved. I ping'ed to the BFCache team on the issue.

Comment 31 by fergal@google.com on Tue, Mar 15, 2022, 8:14 AM EDT Project Member

~~issue 1287996~~ should be fixed now.

Comment 32 by adetaylor@google.com on Fri, Mar 25, 2022, 11:16 AM EDT Project Member

nhiroki@ is your work here now unblocked? Could you update us on your plan?

Comment 33 by adetaylor@google.com on Fri, Mar 25, 2022, 11:17 AM EDT Project Member

(And especially, if this needs to be redirected to the BFCache team, please do so as soon as possible!)

Comment 34 by nhiroki@chromium.org on Sun, Mar 27, 2022, 12:28 PM EDT Project Member

I ran the repro steps on the following version/configuration that contain the fergal@'s fix. It didn't reproduce the original issue or the DCHECK failure.

- 102.0.4968.0 (Developer Build)
- main@{#985731}
- Windows 11 Version 21H2 (Build 22000.556)
- ASAN enabled

sametforuaf@: Sorry to bother you again. Could you check the latest build? Also, I attached a video to show my steps.

crbug1283050.mp4
2.2 MB View Download

Comment 35 by samet...@gmail.com on Sun, Mar 27, 2022, 2:25 PM EDT

Hi nhiroki@, I tested it on version 102.0.4969.0 (Developer Build) (64-bit). It looks fixed now.

Comment 36 by nhiroki@chromium.org on Sun, Mar 27, 2022, 8:12 PM EDT Project Member

Status: Fixed (was: Started)

Thank you for the confirmation!

This should be fixed by https://bugs.chromium.org/p/chromium/issues/detail?id=1287996#c7

Comment 37 by sheriffbot on Mon, Mar 28, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 38 by sheriffbot on Mon, Mar 28, 2022, 1:42 PM EDT Project Member

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

Comment 39 by sheriffbot on Mon, Mar 28, 2022, 2:02 PM EDT Project Member

Labels: Merge-Request-101 Merge-Request-100 Merge-Request-98 Merge-Request-99

This is sufficiently serious that it should be merged to extended stable. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M98. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to stable. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M99. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need

to investigate what - if anything - needs to be merged to M100. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

This is sufficiently serious that it should be merged to dev. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M101. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

Comment 40 by sheriffbot on Mon, Mar 28, 2022, 2:07 PM EDT Project Member

Labels: -Merge-Request-101 Merge-Review-101 Hotlist-Merge-Review

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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

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

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

Comment 41 by sheriffbot on Mon, Mar 28, 2022, 2:07 PM EDT Project Member

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

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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

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

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

Comment 42 by sheriffbot on Mon, Mar 28, 2022, 2:07 PM EDT Project Member

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

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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

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

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

Comment 43 by sheriffbot on Mon, Mar 28, 2022, 2:07 PM EDT Project Member

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

Merge review required: no relevant commits could be automatically detected (via Git Watcher comments), sending to merge review for manual evaluation. If you have not already manually listed the relevant commits to be merged via a comment above, please do so ASAP.

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 44 by mpdenton@chromium.org on Mon, Mar 28, 2022, 4:15 PM EDT Project Member

Owner: fergal@chromium.org
Cc: nhiroki@chromium.org

Assigning fergal@ for merges.

Comment 45 by Git Watcher on Tue, Mar 29, 2022, 4:11 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/a69d2ffadf8420b2625c3337be34905c6c6f88ab

commit a69d2ffadf8420b2625c3337be34905c6c6f88ab
Author: Fergal Daly <fergal@chromium.org>
Date: Tue Mar 29 08:10:17 2022

Switch to use WaitForLoadStop to fix flakiness.

The use of TestNavigationManager was copied from old code.

~~Fixed: 1311145~~,~~1283050~~
Change-Id: I5832708828d3a3a1014a1a03d7af5ee84a952bd9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556259
Reviewed-by: John Abd-El-Malek <jam@chromium.org>
Commit-Queue: Fergal Daly <fergal@chromium.org>
Cr-Commit-Position: refs/heads/main@{#986375}

[modify]
https://crrev.com/a69d2ffadf8420b2625c3337be34905c6c6f88ab/content/browser/back_forward_cache_browsertest.cc

Comment 46 by fergal@google.com on Tue, Mar 29, 2022, 11:19 PM EDT Project Member

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

UAF security bug.

2. What changes specifically would you like to merge? Please link to Gerrit.

https://crrev.com/c/3319862
https://crrev.com/c/3556259

3. Have the changes been released and tested on canary?

First one has. 2nd is a fix to the test to stop flakes, no app code involved but should be merged to ensure the branch tests are stable.

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

no

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.

Maybe. Steps are in https://bugs.chromium.org/p/chromium/issues/detail?id=1283050#c29

Comment 47 by fergal@google.com on Tue, Mar 29, 2022, 11:39 PM EDT Project Member

I've created merges for 99 and 100. The merges had conflicts

https://crrev.com/c/3559270
https://crrev.com/c/3559271

The fix is already in 101

I will also CP the test fix but that it's easier to create that merge after the others land.

Comment 48 by amyressler@chromium.org on Thu, Mar 31, 2022, 2:08 PM EDT Project Member

Labels: -Merge-Review-98 -Merge-Review-99 -Merge-Review-100 -Merge-Review-101 Merge-Approved-101 Merge-Approved-100

Hi fergal@, https://crrev.com/c/3559270 is already in 101, but https://crrev.com/c/3559271 does not appear to have made it to 101 and is only on 102,
so approving merge to 101 for https://crrev.com/c/3559271 and merge to M100 for both fixes

Please merge https://crrev.com/c/3559271 to branch 4951 so this fix can be included in M101 beta.

Please merge both fixes to M100/branch 4896 so these fixes can be included in the next stable respin.

Merge-na for M99 and M99, as M100 is now stable channel and there are no further planned releases of either.

Comment 49 by pbommana@google.com on Fri, Apr 1, 2022, 12:18 PM EDT Project Member

[Bulk Edit] Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch manually asap so that it would be part of next week's M101 Beta release.

Comment 50 by nasko@chromium.org on Fri, Apr 1, 2022, 2:41 PM EDT Project Member

Cc: alex...@chromium.org nasko@chromium.org

~~Issue 1283563~~ has been merged into this issue.

Comment 51 by pbommana@google.com on Mon, Apr 4, 2022, 2:56 PM EDT Project Member

[Bulk Edit]Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch manually asap on or before noon tomorrow so that they would be part of this week's M101 Beta release.

Comment 52 by sheriffbot on Tue, Apr 5, 2022, 12:21 PM EDT Project Member

Cc: amyressler@chromium.org

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

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

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

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

Comment 53 by srinivassista@google.com on Tue, Apr 5, 2022, 1:19 PM EDT Project Member

fergal@ can you please help complete the merges to M100 asap, as we want to re-spin for M100 this week (potentially)

Comment 54 by gov...@chromium.org on Wed, Apr 6, 2022, 5:48 PM EDT Project Member

Please merge your change to M100 branch 4896 ASAP so it can be included in next respin. Thank you.

Comment 55 by Git Watcher on Wed, Apr 6, 2022, 10:17 PM EDT 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/+/57bdd90d8c81168e8f055e5663967854068b7f05

commit 57bdd90d8c81168e8f055e5663967854068b7f05
Author: Fergal Daly <fergal@chromium.org>
Date: Thu Apr 07 02:16:11 2022

Use IsErrorDocument() to prevent BFCacheing of interstitials and errors.

In the bug, a crash occurs because we try to cache an interstitial. We
catch some error documents via status codes etc but interstitials do
not consistently set those. Checking IsErrorDocument() is more reliable.

(cherry picked from commit 7a05b426c6c51254a08de9a8dee8db9c1911b9c9)

~~Bug: 1274308~~,~~1287996~~,~~1283050~~
Change-Id: Ifec662c169c77e33ca5dc4d56b0e42c8d71f1d97
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3319862
Commit-Queue: Fergal Daly <fergal@chromium.org>
Reviewed-by: Rakina Zata Amni <rakina@chromium.org>
Reviewed-by: Andrey Kosyakov <caseq@chromium.org>
Reviewed-by: Alexander Timin <altimin@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#981026}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3559271
Reviewed-by: Hiroki Nakagawa <nhiroki@chromium.org>
Owners-Override: Hiroki Nakagawa <nhiroki@chromium.org>
Commit-Queue: Rakina Zata Amni <rakina@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#1065}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/back_forward_cache_browsertest.cc
[modify]
https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/third_party/blink/public/devtools_protocol/browser_protocol.pdl
[modify]
https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/devtools/protocol/page_handler.cc
[modify]
https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/back_forward_cache_basics_browsertest.cc
[modify]
https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/renderer_host/back_forward_cache_can_store_document_result.cc

[modify] https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/back_forward_cache_browsertest.h
[modify] https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/back_forward_cache_internal_browsertest.cc
[modify] https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/renderer_host/back_forward_cache_impl.cc
[modify] https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/content/browser/renderer_host/back_forward_cache_metrics.h
[modify] https://crrev.com/57bdd90d8c81168e8f055e5663967854068b7f05/base/tracing/protos/chrome_track_event.proto

Comment 56 by sheriffbot on Wed, Apr 6, 2022, 10:19 PM EDT Project Member

Labels: LTS-Merge-Candidate

LTS Milestone M96

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

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

Comment 57 by fergal@google.com on Thu, Apr 7, 2022, 12:32 AM EDT Project Member

I am also CPing the flaky-test fix https://chromium-review.googlesource.com/c/chromium/src/+/3575854

Comment 58 by Git Watcher on Thu, Apr 7, 2022, 1:45 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/80e8d7dbedced3e83a5a754aab69e89c9518ad9f

commit 80e8d7dbedced3e83a5a754aab69e89c9518ad9f
Author: Fergal Daly <fergal@chromium.org>
Date: Thu Apr 07 05:44:20 2022

Switch to use WaitForLoadStop to fix flakiness.

The use of TestNavigationManager was copied from old code.

(cherry picked from commit a69d2ffadf8420b2625c3337be34905c6c6f88ab)

~~Fixed: 1311145~~,~~1283050~~
Change-Id: I5832708828d3a3a1014a1a03d7af5ee84a952bd9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556259
Reviewed-by: John Abd-El-Malek <jam@chromium.org>
Commit-Queue: Fergal Daly <fergal@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3575854
Auto-Submit: Fergal Daly <fergal@chromium.org>

Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Zain Afzal <zafzal@google.com>
Owners-Override: Zain Afzal <zafzal@google.com>
Cr-Commit-Position: refs/branch-heads/4896@{#1066}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/80e8d7dbedced3e83a5a754aab69e89c9518ad9f/content/browser/back_forward_cache_browsertest.cc

Comment 59 by sheriffbot on Fri, Apr 8, 2022, 12:21 PM EDT Project Member

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

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

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

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

Comment 60 by pbommana@google.com on Mon, Apr 11, 2022, 12:38 PM EDT Project Member

[Bulk Edit] Your change has been approved for M101 branch,please go ahead and merge the CL's to M101 branch(http://go/chromebranches) manually asap so that they would be part of this week's first M101 Beta release.

Note : I will be cutting M101 Beta RC build tomorrow around Noon PST, please try to get the changes cherry picked asap.

Comment 61 by rzanoni@google.com on Mon, Apr 11, 2022, 12:49 PM EDT Project Member

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

Comment 62 by amyressler@google.com on Mon, Apr 11, 2022, 1:06 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 63 by amyressler@chromium.org on Mon, Apr 11, 2022, 1:12 PM EDT Project Member

Hello Samet, thank you for this report. As technically this previous issue was already known and reported as a bug (crbug/1274308) we are making an exception and would like to extend a thank you reward as this issue was treated as a security issue in part due to your report. This issue will be duplicated into the pre-existing bug shortly and a similar reward provided for the original submitter. Thank you for your efforts and reporting this issue to us.

Comment 64 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT Project Member

Labels: Release-2-M100

Comment 65 by samet...@gmail.com on Mon, Apr 11, 2022, 1:21 PM EDT

Hi Amy,

I do not agree with the award amount and your decision. Report 1274308 has been publicly reported as a "bug". So the engineers didn't know if there was a safety issue here. This is also a data leak. I politely decline your award.

Thanks!

Comment 66 by amyressler@chromium.org on Mon, Apr 11, 2022, 1:24 PM EDT Project Member

Labels: -Reward-1000 -reward-unpaid reward-declined

Hi Samet, thank you for the response. We understand your decision and will update this issue as reward-declined and will carry on with merging it into the earlier report as earlier mentioned.

Comment 67 by adetaylor@google.com on Mon, Apr 11, 2022, 1:29 PM EDT Project Member

Labels: CVE-2022-1308 CVE_description-missing

Comment 68 by amyressler@chromium.org on Mon, Apr 11, 2022, 4:33 PM EDT Project Member

Status: Duplicate (was: Fixed)
Mergedinto: 1274308

Comment 69 by amyressler@chromium.org on Mon, Apr 11, 2022, 4:42 PM EDT Project Member

Hi Samet, I also wanted to provide additional follow up here that I was remiss in providing in the original response. This VRP reward for this report, even had it been the first report of this issue, would have been significantly reduced since this issue is not web accessible and remote exploitable and is solely reliant on user interaction based on your report. VRP rules state that we reports that are not the first known instance of a report are ineligible for a reward due. Because this showed that there is a security consequence for this issue, mitigated by the a fair amount of user gesture, this issue was allowed to be handled as a security issue and fixed accordingly. The report of the original ~~issue 1274308~~ was highly detailed and provided reproduction steps that allowed this issue to be much easier to reproduce, RCA to be perform, and a fix to be landed and verified. We thought it was only fair that we handle the bugs in this manner and offer a higher 'thank you' reward to each.
We do understand that you are not satisfied with this outcome, but also thought it was good to provide this insight given your response.

Comment 70 by benmason@chromium.org on Wed, Apr 13, 2022, 10:18 AM EDT Project Member

As per comment 47, can we remove the "Merge-Approved-101" label?

Comment 71 by rzanoni@google.com on Mon, Apr 18, 2022, 8:53 AM EDT Project Member

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

Comment 72 by sheriffbot on Mon, Apr 18, 2022, 8:57 AM EDT Project Member

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

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

1. Number of CLs needed for this fix and links to them.

2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 73 by rzanoni@google.com on Mon, Apr 18, 2022, 9:06 AM EDT Project Member

1. 2, https://chromium-review.googlesource.com/q/topic:1283050_4664
2. Low, had to fix unit tests but applying the fix was straightforward
3. https://crrev.com/c/3577265 - 100, https://crrev.com/c/3586816 - 101
4. Yes

Comment 74 by gmpritchard@google.com on Mon, Apr 18, 2022, 10:33 AM EDT Project Member

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

Comment 75 by Git Watcher on Tue, Apr 19, 2022, 10:27 AM EDT Project Member

Status: Fixed (was: Duplicate)
Labels: -merge-approved-101 merge-merged-4951 merge-merged-101
Mergedinto: -1274308

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/fc6dc3985f265602269e60c10916532140eb8a4f

commit fc6dc3985f265602269e60c10916532140eb8a4f
Author: Fergal Daly <fergal@chromium.org>
Date: Tue Apr 19 14:25:57 2022

Switch to use WaitForLoadStop to fix flakiness.

The use of TestNavigationManager was copied from old code.

(cherry picked from commit a69d2ffadf8420b2625c3337be34905c6c6f88ab)

~~Fixed: 1311145~~,~~1283050~~,~~1283050~~
Change-Id: I5832708828d3a3a1014a1a03d7af5ee84a952bd9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556259
Reviewed-by: John Abd-El-Malek <jam@chromium.org>
Commit-Queue: Fergal Daly <fergal@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3558658
Reviewed-by: Ben Mason <benmason@chromium.org>
Commit-Queue: Ben Mason <benmason@chromium.org>
Cr-Commit-Position: refs/branch-heads/4951@{#881}
Cr-Branched-From: 27de6227ca357da0d57ae2c7b18da170c4651438-refs/heads/main@{#982481}

[modify]
https://crrev.com/fc6dc3985f265602269e60c10916532140eb8a4f/content/browser/back_forward_cache_browsertest.cc

Comment 76 by Git Watcher on Tue, Apr 19, 2022, 11:26 AM EDT Project Member

Labels: merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/38ab9c5b06a472fcb5105458b2b4037749c50766

commit 38ab9c5b06a472fcb5105458b2b4037749c50766
Author: Fergal Daly <fergal@chromium.org>
Date: Tue Apr 19 15:25:29 2022

[M96-LTS] Use IsErrorDocument() to prevent BFCacheing of interstitials and errors.

M96 merge issues:
Tests not present on M96:
- back_forward_cache_basics_browsertest.cc
- back_forward_cache_browsertest.h
- back_forward_cache_internal_browsertest.cc
chrome_track_event.proto:
- changed code (tracing) doesn't exist on M96, discarded
all changes
back_forward_cache_browsertest.cc:
- conflicting includes
- removed NavigateAndBlock, which would be called on
on back_forward_cache_browsertest.cc (not present in M96)
page_handler.cc:
- conflicting case statements on NotRestoredReasonToProtocol
back_forward_cache_can_store_document_result.cc:
- NotRestoredReasonToTraceEnum not present on M96
- conflicting case statements on NotRestoredReasonToString
back_forward_cache_metrics.h:
- conflicting entries for NotRestoredReason enum

In the bug, a crash occurs because we try to cache an interstitial. We
catch some error documents via status codes etc but interstitials do
not consistently set those. Checking IsErrorDocument() is more reliable.

(cherry picked from commit 7a05b426c6c51254a08de9a8dee8db9c1911b9c9)

~~Bug: 1274308~~,~~1287996~~,~~1283050~~
Change-Id: Ifec662c169c77e33ca5dc4d56b0e42c8d71f1d97
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3319862
Commit-Queue: Fergal Daly <fergal@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#981026}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3577265
Reviewed-by: Fergal Daly <fergal@chromium.org>
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1592}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/content/browser/back_forward_cache_browsertest.cc
[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/third_party/blink/public/devtools_protocol/browser_prot

ocol.pdl
[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/content/browser/devtools/protocol/page_handler.cc
[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/content/browser/renderer_host/back_forward_cache_can_store_document_result.cc
[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/content/browser/renderer_host/back_forward_cache_impl.cc
[modify]
https://crrev.com/38ab9c5b06a472fcb5105458b2b4037749c50766/content/browser/renderer_host/back_forward_cache_metrics.h

Comment 77 by Git Watcher on Tue, Apr 19, 2022, 12:18 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/7728c580999231f9f8b3202179a293a6b6b65f35

commit 7728c580999231f9f8b3202179a293a6b6b65f35
Author: Roger Zanoni <rzanoni@google.com>
Date: Tue Apr 19 16:17:20 2022

[M96-LTS] Switch to use WaitForLoadStop to fix flakiness.

The use of TestNavigationManager was copied from old code.

~~Fixed: 1311145~~,~~1283050~~
Change-Id: I5832708828d3a3a1014a1a03d7af5ee84a952bd9
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3556259
Commit-Queue: Fergal Daly <fergal@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#986375}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3586816
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1595}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/7728c580999231f9f8b3202179a293a6b6b65f35/content/browser/back_forward_cache_browsertest.cc

Comment 78 by rzanoni@google.com on Tue, Apr 19, 2022, 12:18 PM EDT Project Member

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

Comment 79 by sheriffbot on Tue, Apr 19, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 80 by amyressler@chromium.org on Fri, Apr 22, 2022, 9:55 PM EDT Project Member

Labels: -reward-topanel

adjusting labels from this bug being merged, reopened, then moved back to fixed

Comment 81 by sheriffbot on Sat, Apr 23, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 82 by samet...@gmail.com on Sat, Apr 23, 2022, 4:31 PM EDT

:D

Comment 83 by amyressler@chromium.org on Tue, Apr 26, 2022, 6:43 PM EDT Project Member

Labels: -reward-topanel

the bot has decided to be ornery, so turning over the labels to hopefully correct it--

reward info in comments #62 and #63 (ty for security related contributions for bug for previous report of same issue via ~~issue 1274308~~; ~~issue 1274308~~ provided information and steps to reproduce, allowing for successful reproduction and RCA and this issue displayed security implications of this previously known issue); reward was extended and subsequently declined (comment 65) by researcher; updating labels (again) accordingly

Comment 84 by samet...@gmail.com on Tue, Apr 26, 2022, 6:46 PM EDT

You should try marking this report as duplicate for the bot.

Comment 85 by amyressler@chromium.org on Tue, Apr 26, 2022, 6:51 PM EDT Project Member

Tried that in comment #68 and the git-watcher bot undid that effort in comment #75, so I'm going to play it smart and only war with one bot at a time as to not incur the wrath of our robot overlords.

Comment 86 by sheriffbot on Wed, Apr 27, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 87 by amyressler@chromium.org on Mon, May 2, 2022, 7:50 AM EDT Project Member

Labels: -reward-declined reward-decline

would be helpful if I used the correct label :-|

Comment 88 by amyressler@chromium.org on Mon, May 2, 2022, 10:35 AM EDT Project Member

Labels: -reward-topanel

Comment 89 by sheriffbot on Mon, Jul 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 90 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 91 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing