☆ Starred by 3 users

Owner:	dhvee...@microsoft.com
CC:	adetaylor@chromium.org jun.k...@microsoft.com wychen@chromium.org nyquist@chromium.org pbomm...@chromium.org mdjones@chromium.org amit...@microsoft.com
Status:	Fixed *(Closed)*
Components:	UI>Browser>ReaderMode
Modified:	Aug 26, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
CVE_description-submitted
M-90
Target-90
merge-merged-4240
LTS-Security-86
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
merge-merged-4430_101
Release-3-M90
CVE-2021-30518

Issue 1203590: container-overflow in dom_distiller::TaskTracker::NotifyViewersAndCallbacks

Reported by dhvee...@microsoft.com on Wed, Apr 28, 2021, 3:05 AM EDT Project Member

Code

Chrome Version: 92.0.4492.0
OS: Win10, MacOS

What steps will reproduce the problem?
(1) Compile Chrome ASan build (autogn x64 release is_asan=true)
(2) Open any distiller URL in more than one tab. Trigger navigation as fast as possible. Repro happens when one tab viewer waits for the distillation triggered because of another tab viewer.
(3) Browser crashes

Ex: URL - chrome-distiller://f590a6c2-b165-4813-b69c-4070ac345b10_0034b9eb9949230b74b9f25ab2d02f70c786de48d6e0384f76f8288de23528ac/?time=96683080&url=https%3A%2F%2Fwww.msn.com%2Fen-in%2Fmoney%2Fnews%2Fteslas-elon-musk-calls-for-breakup-of-amazon-in-tweet%2Far-BB154rd0%3Fli%3DAAggbRN

Asan Log -

```
=================================================================
==28172==ERROR: AddressSanitizer: container-overflow on address 0x11f8f69f2ad8 at pc 0x7ffab6d71825 bp 0x007b1cdfe210 sp 0x007b1cdfe258
READ of size 8 at 0x11f8f69f2ad8 thread T0
    #0 0x7ffab6d71824 in dom_distiller::TaskTracker::NotifyViewersAndCallbacks(void) F:\Chromim\src\components\dom_distiller\core\task_tracker.cc:224:21
    #1 0x7ffab6d71489 in dom_distiller::TaskTracker::DistilledArticleReady(class std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct
std::__1::default_delete<class dom_distiller::DistilledArticleProto>>) F:\Chromim\src\components\dom_distiller\core\task_tracker.cc:220:3
    #2 0x7ffab6d6f3f9 in dom_distiller::TaskTracker::OnDistillerFinished(class std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct
std::__1::default_delete<class dom_distiller::DistilledArticleProto>>) F:\Chromim\src\components\dom_distiller\core\task_tracker.cc:156:3
    #3 0x7ffab6d719ae in base::internal::FunctorTraits<void (dom_distiller::TaskTracker::*)
(std::__1::unique_ptr<dom_distiller::DistilledArticleProto,std::__1::default_delete<dom_distiller::DistilledArticleProto> >),void>::Invoke
F:\Chromim\src\base\bind_internal.h:509
    #4 0x7ffab6d719ae in base::internal::InvokeHelper<1,void>::MakeItSo F:\Chromim\src\base\bind_internal.h:668
    #5 0x7ffab6d719ae in base::internal::Invoker<base::internal::BindState<void (dom_distiller::TaskTracker::*)
(std::__1::unique_ptr<dom_distiller::DistilledArticleProto,std::__1::default_delete<dom_distiller::DistilledArticleProto> >),base::WeakPtr<dom_distiller::TaskTracker> >,void
(std::__1::unique_ptr<dom_distiller::DistilledArticleProto,std::__1::default_delete<dom_distiller::DistilledArticleProto> >)>::RunImpl F:\Chromim\src\base\bind_internal.h:721
    #6 0x7ffab6d719ae in base::internal::Invoker<struct base::internal::BindState<void (__cdecl dom_distiller::TaskTracker::*)(class std::__1::unique_ptr<class
dom_distiller::DistilledArticleProto, struct std::__1::default_delete<class dom_distiller::DistilledArticleProto>>), class base::WeakPtr<class dom_distiller::TaskTracker>>, (class
std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct std::__1::default_delete<class dom_distiller::DistilledArticleProto>>)>::RunOnce(class
base::internal::BindStateBase *, class std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct std::__1::default_delete<class dom_distiller::DistilledArticleProto>>
&&) F:\Chromim\src\base\bind_internal.h:690:12
    #7 0x7ffab548f8cc in base::OnceCallback<(class std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct std::__1::default_delete<class
dom_distiller::DistilledArticleProto>>)>::Run(class std::__1::unique_ptr<class dom_distiller::DistilledArticleProto, struct std::__1::default_delete<class
dom_distiller::DistilledArticleProto>>) && F:\Chromim\src\base\callback.h:101:12
    #8 0x7ffab548dde1 in dom_distiller::DistillerImpl::RunDistillerCallbackIfDone(void) F:\Chromim\src\components\dom_distiller\core\distiller.cc:420:29
    #9 0x7ffab548e406 in dom_distiller::DistillerImpl::AddPageIfDone(int) F:\Chromim\src\components\dom_distiller\core\distiller.cc:367:5
    #10 0x7ffab548c216 in dom_distiller::DistillerImpl::OnPageDistillationFinished(int, class GURL const &, class std::__1::unique_ptr<class
dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>>, bool)
F:\Chromim\src\components\dom_distiller\core\distiller.cc:292:3
    #11 0x7ffab548fe21 in base::internal::FunctorTraits<void (dom_distiller::DistillerImpl::*)(int, const GURL &,
std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >, bool),void>::Invoke
F:\Chromim\src\base\bind_internal.h:509
    #12 0x7ffab548fe21 in base::internal::InvokeHelper<1,void>::MakeItSo F:\Chromim\src\base\bind_internal.h:668
    #13 0x7ffab548fe21 in base::internal::Invoker<base::internal::BindState<void (dom_distiller::DistillerImpl::*)(int, const GURL &,
std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >,
bool),base::WeakPtr<dom_distiller::DistillerImpl>,int,GURL>,void
(std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >, bool)>::RunImpl
F:\Chromim\src\base\bind_internal.h:721
    #14 0x7ffab548fe21 in base::internal::Invoker<struct base::internal::BindState<void (__cdecl dom_distiller::DistillerImpl::*)(int, class GURL const &, class
std::__1::unique_ptr<class dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>>, bool), class
base::WeakPtr<class dom_distiller::DistillerImpl>, int, class GURL>, (class std::__1::unique_ptr<class dom_distiller::proto::DomDistillerResult, struct
std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>>, bool)>::Run(class base::internal::BindStateBase *, class std::__1::unique_ptr<class
dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>> &&, bool) F:\Chromim\src\base\bind_internal.h:703:12
    #15 0x7ffab549819a in base::OnceCallback<(class std::__1::unique_ptr<class dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class
dom_distiller::proto::DomDistillerResult>>, bool)>::Run(class std::__1::unique_ptr<class dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class
dom_distiller::proto::DomDistillerResult>>, bool) && F:\Chromim\src\base\callback.h:101:12
    #16 0x7ffab5497ff5 in base::internal::FunctorTraits<base::OnceCallback<void
(std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >, bool)>,void>::Invoke
F:\Chromim\src\base\bind_internal.h:608
    #17 0x7ffab5497ff5 in base::internal::InvokeHelper<0,void>::MakeItSo F:\Chromim\src\base\bind_internal.h:648
    #18 0x7ffab5497ff5 in base::internal::Invoker<base::internal::BindState<base::OnceCallback<void
(std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >,
bool)>,std::__1::unique_ptr<dom_distiller::proto::DomDistillerResult,std::__1::default_delete<dom_distiller::proto::DomDistillerResult> >,bool>,void ()>::RunImpl
F:\Chromim\src\base\bind_internal.h:721
    #19 0x7ffab5497ff5 in base::internal::Invoker<struct base::internal::BindState<class base::OnceCallback<(class std::__1::unique_ptr<class
dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>>, bool)>, class std::__1::unique_ptr<class
dom_distiller::proto::DomDistillerResult, struct std::__1::default_delete<class dom_distiller::proto::DomDistillerResult>>, bool>, (void)>::RunOnce(class
base::internal::BindStateBase *) F:\Chromim\src\base\bind_internal.h:690:12
    #20 0x7ffaabe99e4a in base::OnceCallback<void ()>::Run F:\Chromim\src\base\callback.h:102
    #21 0x7ffaabe99e4a in base::TaskAnnotator::RunTask(char const *, struct base::PendingTask *) F:\Chromim\src\base\task\common\task_annotator.cc:173:33
    #22 0x7ffaae611794 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(class base::sequence_manager::LazyNow *)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:351:25
    #23 0x7ffaae610e19 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork(void)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:264:36
    #24 0x7ffaabf4c230 in base::MessagePumpForUI::DoRunLoop(void) F:\Chromim\src\base\message_loop\message_pump_win.cc:220:67
    #25 0x7ffaabf4a3ef in base::MessagePumpWin::Run(class base::MessagePump::Delegate *) F:\Chromim\src\base\message_loop\message_pump_win.cc:78:3
    #26 0x7ffaae612e70 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, class base::TimeDelta)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460:12
    #27 0x7ffaabe20a03 in base::RunLoop::Run(class base::Location const &) F:\Chromim\src\base\run_loop.cc:133:14
    #28 0x7ffaa55b123f in content::BrowserMainLoop::RunMainMessageLoop(void) F:\Chromim\src\content\browser\browser_main_loop.cc:993:20
    #29 0x7ffaa55b681b in content::BrowserMainRunnerImpl::Run(void) F:\Chromim\src\content\browser\browser_main_runner_impl.cc:152:15
    #30 0x7ffaa55aa8ea in content::BrowserMain(struct content::MainFunctionParams const &) F:\Chromim\src\content\browser\browser_main.cc:47:28
    #31 0x7ffaabbb1608 in content::RunBrowserProcessMain(struct content::MainFunctionParams const &, class content::ContentMainDelegate *)
F:\Chromim\src\content\app\content_main_runner_impl.cc:598:10
    #32 0x7ffaabbb3fa5 in content::ContentMainRunnerImpl::RunBrowser(struct content::MainFunctionParams &, bool)
F:\Chromim\src\content\app\content_main_runner_impl.cc:1081:10
    #33 0x7ffaabbb3171 in content::ContentMainRunnerImpl::Run(bool) F:\Chromim\src\content\app\content_main_runner_impl.cc:956:12
    #34 0x7ffaabbb041e in content::RunContentProcess(struct content::ContentMainParams const &, class content::ContentMainRunner *)
F:\Chromim\src\content\app\content_main.cc:372:36
    #35 0x7ffaabbb0a08 in content::ContentMain(struct content::ContentMainParams const &) F:\Chromim\src\content\app\content_main.cc:398:10
    #36 0x7ffaa1b6145a in ChromeMain F:\Chromim\src\chrome\app\chrome_main.cc:151:12
    #37 0x7ff7a8345bed in MainDllLoader::Launch(struct HINSTANCE__*, class base::TimeTicks) F:\Chromim\src\chrome\app\main_dll_loader_win.cc:169:12
    #38 0x7ff7a8342c47 in main F:\Chromim\src\chrome\app\chrome_exe_main_win.cc:369:20
    #39 0x7ff7a873067f in invoke_main D:\a01\_work\26\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:78
    #40 0x7ff7a873067f in __scrt_common_main_seh D:\a01\_work\26\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
    #41 0x7ffb3cfc7033  (C:\WINDOWS\System32\KERNEL32.DLL+0x180017033)
    #42 0x7ffb3efa2650  (C:\WINDOWS\SYSTEM32\ntdll.dll+0x180052650)

0x11f8f69f2ad8 is located 8 bytes inside of 16-byte region [0x11f8f69f2ad0,0x11f8f69f2ae0)
allocated by thread T0 here:
    #0 0x7ff7a83e3ffb in malloc C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_malloc_win.cpp:98
    #1 0x7ffabe2218be in operator new(unsigned __int64) D:\a01\_work\26\s\src\vctools\crt\vcstartup\src\heap\new_scalar.cpp:35
    #2 0x7ffab6d7200b in std::__1::__libcpp_operator_new F:\Chromim\src\buildtools\third_party\libc++\trunk\include\new:235
    #3 0x7ffab6d7200b in std::__1::__libcpp_allocate F:\Chromim\src\buildtools\third_party\libc++\trunk\include\new:261
    #4 0x7ffab6d7200b in std::__1::allocator<dom_distiller::ViewRequestDelegate *>::allocate F:\Chromim\src\buildtools\third_party\libc++\trunk\include\memory:778
    #5 0x7ffab6d7200b in std::__1::allocator_traits<std::__1::allocator<dom_distiller::ViewRequestDelegate *> >::allocate
F:\Chromim\src\buildtools\third_party\libc++\trunk\include\__memory\allocator_traits.h:260
    #6 0x7ffab6d7200b in std::__1::__split_buffer<dom_distiller::ViewRequestDelegate *,std::__1::allocator<dom_distiller::ViewRequestDelegate *> &>::__split_buffer
F:\Chromim\src\buildtools\third_party\libc++\trunk\include\__split_buffer:315
    #7 0x7ffab6d7200b in std::__1::vector<class dom_distiller::ViewRequestDelegate *, class std::__1::allocator<class dom_distiller::ViewRequestDelegate
*>>::__push_back_slow_path<class dom_distiller::ViewRequestDelegate *const &>(class dom_distiller::ViewRequestDelegate *const &)
F:\Chromim\src\buildtools\third_party\libc++\trunk\include\vector:1624:49
    #8 0x7ffab6d6fd2d in std::__1::vector<dom_distiller::ViewRequestDelegate *,std::__1::allocator<dom_distiller::ViewRequestDelegate *> >::push_back
F:\Chromim\src\buildtools\third_party\libc++\trunk\include\vector:1641
    #9 0x7ffab6d6fd2d in dom_distiller::TaskTracker::AddViewer(class dom_distiller::ViewRequestDelegate *)
F:\Chromim\src\components\dom_distiller\core\task_tracker.cc:90:12
    #10 0x7ffab547051f in dom_distiller::DomDistillerService::ViewUrl(class dom_distiller::ViewRequestDelegate *, class std::__1::unique_ptr<class dom_distiller::DistillerPage,
struct std::__1::default_delete<class dom_distiller::DistillerPage>>, class GURL const &) F:\Chromim\src\components\dom_distiller\core\dom_distiller_service.cc:71:21
    #11 0x7ffab60d7762 in dom_distiller::LazyDomDistillerService::ViewUrl(class dom_distiller::ViewRequestDelegate *, class std::__1::unique_ptr<class
dom_distiller::DistillerPage, struct std::__1::default_delete<class dom_distiller::DistillerPage>>, class GURL const &)
F:\Chromim\src\chrome\browser\dom_distiller\lazy_dom_distiller_service.cc:40:21
    #12 0x7ffab8eedec6 in dom_distiller::viewer::CreateViewRequest(class dom_distiller::DomDistillerServiceInterface *, class GURL const &, class
dom_distiller::ViewRequestDelegate *, class gfx::Size const &) F:\Chromim\src\components\dom_distiller\core\viewer.cc:327:35
    #13 0x7ffab60da3d4 in dom_distiller::DomDistillerViewerSource::StartDataRequest(class GURL const &, class base::RepeatingCallback<(void)> const &, class
base::OnceCallback<(class scoped_refptr<class base::RefCountedMemory>)>)
F:\Chromim\src\components\dom_distiller\content\browser\dom_distiller_viewer_source.cc:255:49
    #14 0x7ffaa654b86d in content::`anonymous namespace'::StartURLLoader F:\Chromim\src\content\browser\webui\web_ui_url_loader_factory.cc:204:21
    #15 0x7ffaa654a07c in content::`anonymous namespace'::WebUIURLLoaderFactory::CreateLoaderAndStart
F:\Chromim\src\content\browser\webui\web_ui_url_loader_factory.cc:300:5
    #16 0x7ffaa36df8fb in network::mojom::URLLoaderFactoryStubDispatch::Accept(class network::mojom::URLLoaderFactory *, class mojo::Message *)
F:\Chromim\src\out\release_x64\gen\services\network\public\mojom\url_loader_factory.mojom.cc:237:13
    #17 0x7ffaac2faa61 in mojo::InterfaceEndpointClient::HandleValidatedMessage(class mojo::Message *)
F:\Chromim\src\mojo\public\cpp\bindings\lib\interface_endpoint_client.cc:849:54
    #18 0x7ffaaea5bc71 in mojo::MessageDispatcher::Accept(class mojo::Message *) F:\Chromim\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:48:24
    #19 0x7ffaac310844 in mojo::internal::MultiplexRouter::ProcessIncomingMessage(class mojo::internal::MultiplexRouter::MessageWrapper *, enum
mojo::internal::MultiplexRouter::ClientCallBehavior, class base::SequencedTaskRunner *) F:\Chromim\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:1023:42
    #20 0x7ffaac30f8d8 in mojo::internal::MultiplexRouter::Accept(class mojo::Message *) F:\Chromim\src\mojo\public\cpp\bindings\lib\multiplex_router.cc:690:7
    #21 0x7ffaaea5bd5e in mojo::MessageDispatcher::Accept(class mojo::Message *) F:\Chromim\src\mojo\public\cpp\bindings\lib\message_dispatcher.cc:43:19
    #22 0x7ffaac2f5631 in mojo::Connector::DispatchMessageW(class mojo::Message) F:\Chromim\src\mojo\public\cpp\bindings\lib\connector.cc:522:49
    #23 0x7ffaac2f6daa in mojo::Connector::ReadAllAvailableMessages(void) F:\Chromim\src\mojo\public\cpp\bindings\lib\connector.cc:580:14
    #24 0x7ffaac3450fe in base::RepeatingCallback<void (unsigned int, const mojo::HandleSignalsState &)>::Run F:\Chromim\src\base\callback.h:169
    #25 0x7ffaac3450fe in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, struct mojo::HandleSignalsState const &)
F:\Chromim\src\mojo\public\cpp\system\simple_watcher.cc:278:14
```

```
    #26 0x7ffaabe99e4a in base::OnceCallback<void ()>::Run F:\Chromim\src\base\callback.h:102
    #27 0x7ffaabe99e4a in base::TaskAnnotator::RunTask(char const *, struct base::PendingTask *) F:\Chromim\src\base\task\common\task_annotator.cc:173:33
    #28 0x7ffaae611794 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(class base::sequence_manager::LazyNow *)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:351:25
    #29 0x7ffaae610e19 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork(void)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:264:36
    #30 0x7ffaabf4c230 in base::MessagePumpForUI::DoRunLoop(void) F:\Chromim\src\base\message_loop\message_pump_win.cc:220:67
    #31 0x7ffaabf4a3ef in base::MessagePumpWin::Run(class base::MessagePump::Delegate *) F:\Chromim\src\base\message_loop\message_pump_win.cc:78:3
    #32 0x7ffaae612e70 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, class base::TimeDelta)
F:\Chromim\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460:12
    #33 0x7ffaabe20a03 in base::RunLoop::Run(class base::Location const &) F:\Chromim\src\base\run_loop.cc:133:14
    #34 0x7ffaa55b123f in content::BrowserMainLoop::RunMainMessageLoop(void) F:\Chromim\src\content\browser\browser_main_loop.cc:993:20
    #35 0x7ffaa55b681b in content::BrowserMainRunnerImpl::Run(void) F:\Chromim\src\content\browser\browser_main_runner_impl.cc:152:15
    #36 0x7ffaa55aa8ea in content::BrowserMain(struct content::MainFunctionParams const &) F:\Chromim\src\content\browser\browser_main.cc:47:28

HINT: if you don't care about these errors you may set ASAN_OPTIONS=detect_container_overflow=0.
If you suspect a false positive see also: https://github.com/google/sanitizers/wiki/AddressSanitizerContainerOverflow.
SUMMARY: AddressSanitizer: container-overflow F:\Chromim\src\components\dom_distiller\core\task_tracker.cc:224:21 in
dom_distiller::TaskTracker::NotifyViewersAndCallbacks(void)
Shadow bytes around the buggy address:
  0x0434153be500: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0434153be510: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0434153be520: fa fa fd fd fa fa fd fd fa fa fd fd fa fa fd fd
  0x0434153be530: fa fa fd fa fa fa fd fd fa fa fd fd fa fa fd fa
  0x0434153be540: fa fa fd fa fa fa fd fa fa fa 00 00 fa fa fd fd
=>0x0434153be550: fa fa fd fd fa fa fd fa fa fa 00[fc]fa fa 00 fa
  0x0434153be560: fa fa fd fd fa fa fd fa fa fa fd fa fa fa fd fa
  0x0434153be570: fa fa fd fa fa fa fd fa fa fa fd fa fa fa fd fa
  0x0434153be580: fa fa fd fa fa fa fd fa fa fa fd fd fa fa fd fa
  0x0434153be590: fa fa fd fa fa fa 00 fa fa fa 00 fa fa fa 00 fa
  0x0434153be5a0: fa fa 00 fa fa fa 00 fa fa fa 00 fa fa fa 00 00
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
==28172==ABORTING
```

Comment 1 by dhvee...@microsoft.com on Wed, Apr 28, 2021, 3:25 AM EDT Project Member

Root cause -

PFA for detailed flow as to why there is container overflow..

Summary -

* If there are multiple viewers with TaskTracker, when distilled article is ready while notifying the viewers we are indirectly erasing viewers from vector while iterating.

TaskTracker::DistilledArticleReady ->
TaskTracker::NotifyViewersAndCallbacks(Iterating over viewers) ->
DomDistillerRequestViewBase::OnArticleReady ->
ViewerHandle::~ViewerHandle ->
TaskTracker::RemoveViewer(erasing viewer from vector while iterating) ->

Fix -
Replace vector with ObserverList that is safe to modify while iterating. Verified that all required calls are made in same thread - BrowserMain i.e. ObserverList is enough, no need to use ObserverListThreadSafe.

P.S -

* The repro steps added in the bug is one of the use-cases. The crash will occur in any situation when TaskTracker holds more than one viewer.

security_bug_drawio (1).png
95.6 KB View Download

Comment 2 by ajgo@google.com on Wed, Apr 28, 2021, 11:18 AM EDT Project Member

Cc: mdjones@chromium.org nyquist@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable Pri-2

adding some labels. dhveerap - are you working on a fix?

Comment 3 by dhvee...@microsoft.com on Wed, Apr 28, 2021, 11:44 AM EDT Project Member

ajgo - I rasied a CL https://chromium-review.googlesource.com/c/chromium/src/+/2856118

Comment 4 by ajgo@google.com on Wed, Apr 28, 2021, 5:55 PM EDT Project Member

Labels: -Security_Severity-Medium Security_Severity-High

Great! Please mark this issue as Fixed once the CL is merged to `main` so that we can consider merging to older branches.

(marking as High as it's a browser UAF - the amount of user interaction might make it less severe)

Comment 5 by Git Watcher on Thu, Apr 29, 2021, 11:53 AM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/be19f42dab0706d5fdd74acd6eaa424e9277e9c4

commit be19f42dab0706d5fdd74acd6eaa424e9277e9c4
Author: Akhila Veerapuraju <dhveerap@microsoft.com>
Date: Thu Apr 29 15:52:19 2021

Replace std::vector with base::ObserverList to support container modification while iterating

TaskTracker saves list of viewers in vector, that needs to be notified
when distillation is completed. At the time of notifying the viewers,
we are indirectly erasing viewers from vector while iterating.

This is causing container-overflow in asan build when vector has more
than one viewer while notifying.

This change is to replace vector with ObserverList that can be modified
during iteration without invalidating the iterator.

~~Bug: 1203590~~
Change-Id: I7c7b8237584c48c9ebc2639b9268a6a78c2db4b2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2856118
Reviewed-by: Matt Jones <mdjones@chromium.org>
Commit-Queue: Akhila Veerapuraju <dhveerap@microsoft.com>
Cr-Commit-Position: refs/heads/master@{#877492}

[modify] https://crrev.com/be19f42dab0706d5fdd74acd6eaa424e9277e9c4/components/dom_distiller/core/task_tracker.cc
[modify] https://crrev.com/be19f42dab0706d5fdd74acd6eaa424e9277e9c4/components/dom_distiller/core/task_tracker.h

Comment 6 by dhvee...@microsoft.com on Thu, Apr 29, 2021, 11:59 AM EDT Project Member

Status: Fixed (was: Started)

Comment 7 by sheriffbot on Thu, Apr 29, 2021, 12:47 PM EDT Project Member

Labels: M-90 Target-90

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 8 by sheriffbot on Thu, Apr 29, 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 9 by sheriffbot on Thu, Apr 29, 2021, 2:02 PM EDT Project Member

Labels: Restrict-View-SecurityNotify

Comment 10 by sheriffbot on Thu, Apr 29, 2021, 2:22 PM EDT Project Member

Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (877492) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (877492) appears to be after beta branch point (870763).

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

Comment 11 by sheriffbot on Fri, Apr 30, 2021, 11:58 AM EDT Project Member

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91's targeted beta branch promotion date has already passed, so this requires manual review
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/+/master/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: benmason@(Android), bindusuvarna@(iOS), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 12 by pbommana@google.com on Fri, Apr 30, 2021, 3:08 PM EDT Project Member

Cc: adetaylor@chromium.org pbomm...@chromium.org

+Adetaylor(Security TPM) for review.

Comment 13 by adetaylor@google.com on Mon, May 3, 2021, 11:08 AM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91, please merge to branch 4472.

Comment 14 by dhvee...@microsoft.com on Mon, May 3, 2021, 11:56 PM EDT Project Member

adetaylor/ajgo Should I manually create a CL to 4472 or bot will do on adding the label Merge-Approved-91?

Comment 15 by ajgo@google.com on Mon, May 3, 2021, 11:59 PM EDT Project Member

Yes, please make a CL targetting 4472 - the gerrit ui should have a button that helps with that.

Comment 16 by dhvee...@microsoft.com on Tue, May 4, 2021, 12:34 AM EDT Project Member ajgo - Done

2870968: [Merge 91] Replace std::vector with base::ObserverList to support container modification while iterating | https://chromium-review.googlesource.com/c/chromium/src/+/2870968

Comment 17 by pbommana@google.com on Tue, May 4, 2021, 7:08 AM EDT Project Member

[Bulk Edit] Your change has been approved for M91. Please go ahead and merge the CL to branch 4472 (refs/branch-heads/4472) manually asap so that it would be part of tomorrow's Beta release.

Comment 18 by Git Watcher on Tue, May 4, 2021, 9:28 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/+/97ef1ed58e105ad9dfaaec44db27c326112756e7

commit 97ef1ed58e105ad9dfaaec44db27c326112756e7
Author: Akhila Veerapuraju <dhveerap@microsoft.com>
Date: Tue May 04 13:27:26 2021

[Merge 91] Replace std::vector with base::ObserverList to support container modification while iterating

TaskTracker saves list of viewers in vector, that needs to be notified
when distillation is completed. At the time of notifying the viewers,
we are indirectly erasing viewers from vector while iterating.

This is causing container-overflow in asan build when vector has more
than one viewer while notifying.

This change is to replace vector with ObserverList that can be modified
during iteration without invalidating the iterator.

(cherry picked from commit be19f42dab0706d5fdd74acd6eaa424e9277e9c4)

~~Bug: 1203590~~
Change-Id: I7c7b8237584c48c9ebc2639b9268a6a78c2db4b2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2856118
Reviewed-by: Matt Jones <mdjones@chromium.org>
Commit-Queue: Akhila Veerapuraju <dhveerap@microsoft.com>
Cr-Original-Commit-Position: refs/heads/master@{#877492}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2870968
Cr-Commit-Position: refs/branch-heads/4472@{#721}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/97ef1ed58e105ad9dfaaec44db27c326112756e7/components/dom_distiller/core/task_tracker.cc
[modify] https://crrev.com/97ef1ed58e105ad9dfaaec44db27c326112756e7/components/dom_distiller/core/task_tracker.h

Comment 19 by adetaylor@google.com on Tue, May 4, 2021, 12:47 PM EDT Project Member

Labels: -Merge-Request-90 Merge-Approved-90

Approving merge to M90, branch 4430. Please merge by EOD PST Thursday for inclusion in next week's security refresh.

Comment 20 by Git Watcher on Thu, May 6, 2021, 11:45 AM EDT Project Member

Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/bdd2fc10e7ae2008ffd57385f1f159c315d4cb0a

commit bdd2fc10e7ae2008ffd57385f1f159c315d4cb0a
Author: Akhila Veerapuraju <dhveerap@microsoft.com>
Date: Thu May 06 15:44:39 2021

[Merge 90] Replace std::vector with base::ObserverList to support container modification while iterating

TaskTracker saves list of viewers in vector, that needs to be notified
when distillation is completed. At the time of notifying the viewers,
we are indirectly erasing viewers from vector while iterating.

This is causing container-overflow in asan build when vector has more
than one viewer while notifying.

This change is to replace vector with ObserverList that can be modified
during iteration without invalidating the iterator.

(cherry picked from commit be19f42dab0706d5fdd74acd6eaa424e9277e9c4)

~~Bug: 1203590~~
Change-Id: I7c7b8237584c48c9ebc2639b9268a6a78c2db4b2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2856118
Reviewed-by: Matt Jones <mdjones@chromium.org>
Commit-Queue: Akhila Veerapuraju <dhveerap@microsoft.com>
Cr-Original-Commit-Position: refs/heads/master@{#877492}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2872685
Cr-Commit-Position: refs/branch-heads/4430@{#1408}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/bdd2fc10e7ae2008ffd57385f1f159c315d4cb0a/components/dom_distiller/core/task_tracker.cc
[modify] https://crrev.com/bdd2fc10e7ae2008ffd57385f1f159c315d4cb0a/components/dom_distiller/core/task_tracker.h

Comment 21 by amyressler@chromium.org on Fri, May 7, 2021, 5:06 PM EDT Project Member

Labels: Release-3-M90

Comment 22 by vsavu@google.com on Mon, May 10, 2021, 9:32 AM EDT Project Member

Labels: LTS-Security-86 LTS-Merge-Request-86

Comment 23 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT Project Member

Labels: CVE-2021-30518 CVE_description-missing

Comment 24 by amyressler@chromium.org on Mon, May 10, 2021, 11:09 AM EDT Project Member

Hi dhveerap@ - by what name/title/handle would you like to be credited for this issue?

Comment 25 by dhvee...@microsoft.com on Mon, May 10, 2021, 11:21 AM EDT Project Member
amyressler - This was found in Microsoft Edge by Jun.

Please credit - Jun Kokatsu, Microsoft Browser Vulnerability Research

Comment 26 by gianluca@google.com on Wed, May 12, 2021, 12:15 PM EDT Project Member
Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 27 by Git Watcher on Tue, May 18, 2021, 12:27 PM EDT Project Member
Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f8018baa9357078c04883077c14cdb363153656d

commit f8018baa9357078c04883077c14cdb363153656d
Author: Akhila Veerapuraju <dhveerap@microsoft.com>
Date: Tue May 18 16:26:00 2021

Replace std::vector with base::ObserverList to support container modification while iterating

TaskTracker saves list of viewers in vector, that needs to be notified
when distillation is completed. At the time of notifying the viewers,
we are indirectly erasing viewers from vector while iterating.

This is causing container-overflow in asan build when vector has more
than one viewer while notifying.

This change is to replace vector with ObserverList that can be modified
during iteration without invalidating the iterator.

(cherry picked from commit be19f42dab0706d5fdd74acd6eaa424e9277e9c4)

~~Bug: 1203590~~
Change-Id: I7c7b8237584c48c9ebc2639b9268a6a78c2db4b2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2856118
Reviewed-by: Matt Jones <mdjones@chromium.org>
Commit-Queue: Akhila Veerapuraju <dhveerap@microsoft.com>
Cr-Original-Commit-Position: refs/heads/master@{#877492}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883743
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1644}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/f8018baa9357078c04883077c14cdb363153656d/components/dom_distiller/core/task_tracker.cc
[modify] https://crrev.com/f8018baa9357078c04883077c14cdb363153656d/components/dom_distiller/core/task_tracker.h

Comment 28 by Git Watcher on Thu, May 20, 2021, 7:02 AM EDT Project Member
Labels: merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/882163473f4a73e80c5f9064b589a669a9a68db1

commit 882163473f4a73e80c5f9064b589a669a9a68db1
Author: Akhila Veerapuraju <dhveerap@microsoft.com>
Date: Thu May 20 10:59:16 2021

[Merge 90] Replace std::vector with base::ObserverList to support container modification while iterating

TaskTracker saves list of viewers in vector, that needs to be notified
when distillation is completed. At the time of notifying the viewers,
we are indirectly erasing viewers from vector while iterating.

This is causing container-overflow in asan build when vector has more
than one viewer while notifying.

This change is to replace vector with ObserverList that can be modified
during iteration without invalidating the iterator.

(cherry picked from commit be19f42dab0706d5fdd74acd6eaa424e9277e9c4)

(cherry picked from commit bdd2fc10e7ae2008ffd57385f1f159c315d4cb0a)

~~Bug: 1203590~~
Change-Id: I7c7b8237584c48c9ebc2639b9268a6a78c2db4b2
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2856118
Reviewed-by: Matt Jones <mdjones@chromium.org>
Commit-Queue: Akhila Veerapuraju <dhveerap@microsoft.com>
Cr-Original-Original-Commit-Position: refs/heads/master@{#877492}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2872685
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1408}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884088
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430_101@{#40}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/882163473f4a73e80c5f9064b589a669a9a68db1/components/dom_distiller/core/task_tracker.cc
[modify] https://crrev.com/882163473f4a73e80c5f9064b589a669a9a68db1/components/dom_distiller/core/task_tracker.h

Comment 29 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member
Labels: -CVE_description-missing CVE_description-submitted

Comment 30 by sheriffbot on Thu, Aug 26, 2021, 1:30 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

About Monorail User Guide Release Notes Feedback on Monorail Terms Privacy