☆ Starred by 4 users

Owner:	ricea@chromium.org **OOO until January 5th**
CC:	yukishiino@chromium.org mlippautz@chromium.org yhirano@chromium.org adetaylor@chromium.org fergal@chromium.org haraken@chromium.org vahl@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Network>WebSockets Blink>GarbageCollection
Modified:	Sep 16, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-01-31
OS:	Linux
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
reward-5000
Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-89
Target-89
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
merge-merged-4324
merge-merged-88
external_security_report
merge-merged-4389
merge-merged-89

Issue 1170657: use after poison in DOMWebSocket

Reported by nekla...@gmail.com on Tue, Jan 26, 2021, 3:09 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.141 Safari/537.36

Steps to reproduce the problem:
OS:
Ubuntu 20.04
Chromium 89.0.4350.4(asan build)
Chromium 90.0.4399.0(asan build)
1. unzip poc.zip
2. python3.8 -m http.server 8000
3. chrome --js-flags=--expose-gc --user-data-dir=/tmp/x2 http://localhost:8000/crash2/main.html

After the print dialog appears, manually click Refresh, and it will repro immediately.
By the way, do not use http://127.0.0.1:8000/crash2/main.html

What is the expected behavior?

What went wrong?

```
==1==ERROR: AddressSanitizer: use-after-poison on address 0x7ec2c85c9130 at pc 0x5609d41f3e98 bp 0x7ffc9ca6bfc0 sp 0x7ffc9ca6bfb8
WRITE of size 8 at 0x7ec2c85c9130 thread T0 (chrome)
error: unknown argument '--demangle=True'
    #0 0x5609d41f3e97 in WTF::AtomicMemzero(void*, unsigned long) ./../../buildtools/third_party/libc++/trunk/include/atomic:957
    #1 0x5609d41f3e97 in store ./../../buildtools/third_party/libc++/trunk/include/atomic:1479
    #2 0x5609d41f3e97 in AtomicMemzero ./../../third_party/blink/renderer/platform/wtf/allocator/allocator.cc:65
    #3 0x5609d41f3e97 in ?? ??:0
    #4 0x5609e22894ba in blink::DOMWebSocket::EventQueue::ContextDestroyed() ./../../third_party/blink/renderer/platform/wtf/deque.h:?
    #5 0x5609e22894ba in clear ./../../third_party/blink/renderer/platform/wtf/deque.h:455
    #6 0x5609e22894ba in ContextDestroyed ./../../third_party/blink/renderer/modules/websockets/dom_websocket.cc:130
    #7 0x5609e22894ba in ?? ??:0
    #8 0x5609cd55ef2f in blink::NormalPage::ToBeFinalizedObject::Finalize() ./../../third_party/blink/renderer/platform/heap/impl/heap_page.cc:95
    #9 0x5609cd55ef2f in Finalize ./../../third_party/blink/renderer/platform/heap/impl/heap_page.cc:1402
    #10 0x5609cd55ef2f in ?? ??:0
    #11 0x5609cd5603bb in blink::NormalPage::Sweep(blink::FinalizeType) ./../../third_party/blink/renderer/platform/heap/impl/heap_page.cc:1513
    #12 0x5609cd5603bb in ?? ??:0
    #13 0x5609cd556126 in blink::BaseArena::SweepUnsweptPage(blink::BasePage*) ./../../third_party/blink/renderer/platform/heap/impl/heap_page.cc:311
    #14 0x5609cd556126 in ?? ??:0
    #15 0x5609cd557d61 in blink::BaseArena::CompleteSweep() ./../../third_party/blink/renderer/platform/heap/impl/heap_page.cc:407
    #16 0x5609cd557d61 in ?? ??:0
    #17 0x5609cd5454f6 in blink::ThreadHeap::CompleteSweep() ./../../third_party/blink/renderer/platform/heap/impl/heap.cc:709
    #18 0x5609cd5454f6 in ?? ??:0
    #19 0x5609cd575697 in blink::ThreadState::CompleteSweep() ./../../third_party/blink/renderer/platform/heap/impl/thread_state.cc:738
    #20 0x5609cd575697 in ?? ??:0
    #21 0x5609cd5827ce in blink::ThreadState::AtomicPauseSweepAndCompact(blink::BlinkGC::CollectionType, blink::BlinkGC::MarkingType, blink::BlinkGC::SweepingType)
./../../third_party/blink/renderer/platform/heap/impl/thread_state.cc:1355
    #22 0x5609cd5827ce in ?? ??:0
    #23 0x5609cd586e77 in blink::UnifiedHeapController::TraceEpilogue(v8::EmbedderHeapTracer::TraceSummary*)
./../../third_party/blink/renderer/platform/heap/impl/unified_heap_controller.cc:93
    #24 0x5609cd586e77 in ?? ??:0
    #25 0x5609cb60bb82 in v8::internal::LocalEmbedderHeapTracer::TraceEpilogue() ./../../v8/src/heap/embedder-tracing.cc:35
    #26 0x5609cb60bb82 in ?? ??:0
    #27 0x5609cb69291b in v8::internal::Heap::PerformGarbageCollection(v8::internal::GarbageCollector, v8::GCCallbackFlags) ./../../v8/src/heap/heap.cc:2082
    #28 0x5609cb69291b in ?? ??:0
    #29 0x5609cb68a0ee in v8::internal::Heap::CollectGarbage(v8::internal::AllocationSpace, v8::internal::GarbageCollectionReason, v8::GCCallbackFlags)
./../../v8/src/heap/heap.cc:1620
    #30 0x5609cb68a0ee in ?? ??:0
    #31 0x5609cb68f03b in v8::internal::Heap::PreciseCollectAllGarbage(int, v8::internal::GarbageCollectionReason, v8::GCCallbackFlags) ./../../v8/src/heap/heap.cc:1312
    #32 0x5609cb68f03b in PreciseCollectAllGarbage ./../../v8/src/heap/heap.cc:1443
    #33 0x5609cb68f03b in ?? ??:0
    #34 0x5609cd579bb5 in blink::ThreadState::CollectAllGarbageForTesting(blink::BlinkGC::StackState)
./../../third_party/blink/renderer/platform/heap/impl/thread_state.cc:1620
    #35 0x5609cd579bb5 in ?? ??:0
    #36 0x5609cd57de32 in blink::ThreadState::SafePoint(blink::BlinkGC::StackState) ./../../third_party/blink/renderer/platform/heap/impl/thread_state.cc:634
    #37 0x5609cd57de32 in SafePoint ./../../third_party/blink/renderer/platform/heap/impl/thread_state.cc:943
    #38 0x5609cd57de32 in ?? ??:0
    #39 0x5609ce888c8c in
base::sequence_manager::internal::SequenceManagerImpl::NotifyDidProcessTask(base::sequence_manager::internal::SequenceManagerImpl::ExecutingTask*,
base::sequence_manager::LazyNow*) ./../../base/task/sequence_manager/sequence_manager_impl.cc:875
    #40 0x5609ce888c8c in ?? ??:0
    #41 0x5609ce88813c in base::sequence_manager::internal::SequenceManagerImpl::DidRunTask() ./../../base/task/sequence_manager/sequence_manager_impl.cc:677
    #42 0x5609ce88813c in ?? ??:0
    #43 0x5609ce8b69ea in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:356
    #44 0x5609ce8b69ea in ?? ??:0
    #45 0x5609ce8b60d4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:264
    #46 0x5609ce8b60d4 in ?? ??:0
    #47 0x5609ce77b910 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) ./../../base/message_loop/message_pump_default.cc:39
    #48 0x5609ce77b910 in ?? ??:0
    #49 0x5609ce8b818c in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
./../../base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:460
    #50 0x5609ce8b818c in ?? ??:0
    #51 0x5609ce801f61 in base::RunLoop::Run(base::Location const&) ./../../base/run_loop.cc:133
    #52 0x5609ce801f61 in ?? ??:0
    #53 0x5609e330a539 in content::RendererMain(content::MainFunctionParams const&) ./../../content/renderer/renderer_main.cc:260
    #54 0x5609e330a539 in ?? ??:0
    #55 0x5609ce55ba0d in content::RunZygote(content::ContentMainDelegate*) ./../../content/app/content_main_runner_impl.cc:534
    #56 0x5609ce55ba0d in ?? ??:0
    #57 0x5609ce55ee99 in content::ContentMainRunnerImpl::Run(bool) ./../../content/app/content_main_runner_impl.cc:937
    #58 0x5609ce55ee99 in ?? ??:0
    #59 0x5609ce558e7e in content::RunContentProcess(content::ContentMainParams const&, content::ContentMainRunner*) ./../../content/app/content_main.cc:372
    #60 0x5609ce558e7e in ?? ??:0
    #61 0x5609ce55946c in content::ContentMain(content::ContentMainParams const&) ./../../content/app/content_main.cc:398
    #62 0x5609ce55946c in ?? ??:0
    #63 0x5609c23ae727 in ChromeMain ./../../chrome/app/chrome_main.cc:141
    #64 0x5609c23ae727 in ?? ??:0
error: unknown argument '--demangle=True'
    #65 0x7f881e68c0b2 in __libc_start_main ??:?
    #66 0x7f881e68c0b2 in ?? ??:0
```

Address 0x7ec2c85c9130 is a wild pointer.

Did this work before? N/A

Chrome version: 90.0.4399.0 Channel: dev
OS Version: 20.04
Flash Version:

[Deleted] **poc.zip**

Comment 1 by sheriffbot on Tue, Jan 26, 2021, 3:12 AM EST Project Member

Labels: external_security_report

Comment 2 by rsleevi@chromium.org on Tue, Jan 26, 2021, 8:47 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: haraken@chromium.org
Labels: Security_Severity-Medium Security_Impact-Head
Components: Blink>MemoryAllocator>GarbageCollection

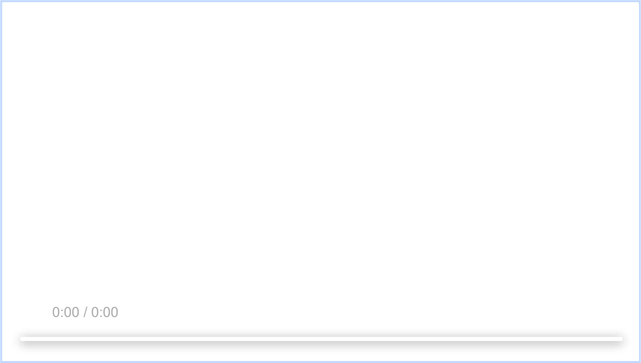
Thanks! I was able to reproduce this using asan-linux-release-847401

The need for manual interaction means this is Medium, as described at https://chromium.googlesource.com/chromium/src/+/master/docs/security/severity-guidelines.md , although it would be useful if you can identify a scenario where this doesn't require interaction.

I'm setting Sec-Impacts_Head for now, because I haven't had a chance to bisect this through the releases.

haraken@: Could you take a look at this?

test.webm
1.6 KB View Download



testharness.js
141 KB View Download

submit
175 bytes View Download

main.html
56 bytes View Download

crash.html
548 bytes View Download

Comment 3 by haraken@google.com on Tue, Jan 26, 2021, 9:16 PM EST Project Member

Owner: ricea@chromium.org
Components: Blink>Network>WebSockets

ricea: Would you take a look at this bug? It looks happening in websocket code.

Comment 4 by haraken@google.com on Tue, Jan 26, 2021, 9:16 PM EST Project Member

Cc: haraken@chromium.org

Comment 5 by ricea@chromium.org on Tue, Jan 26, 2021, 9:49 PM EST Project Member

I think we can probably fix it just by not explicitly clearing the |events_| member. It should eventually get garbage collected anyway.
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/websockets/dom_websocket.h;l=194?q=EventQueue::events_&ss=chromium%2Fchromium%2Fsrc

Or does the HeapDeque need to be explicitly destroyed?

Comment 6 by sheriffbot on Wed, Jan 27, 2021, 1:08 PM EST Project Member

Labels: Target-89 M-89

Setting milestone and target because of Security_Impact=Head and medium severity.

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

Comment 7 by sheriffbot on Wed, Jan 27, 2021, 1:18 PM EST Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 8 by sheriffbot on Wed, Jan 27, 2021, 1:39 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 ricea@chromium.org on Wed, Jan 27, 2021, 9:58 PM EST Project Member

Status: Started (was: Assigned)

#7 I'm working on a fix. As far as I know this vulnerability has been present for years, so there's nothing we can revert.

Comment 10 by rsleevi@chromium.org on Wed, Jan 27, 2021, 11:27 PM EST Project Member

Labels: -Security_Impact-Head -ReleaseBlock-Stable Security_Impact-Stable

Thanks Adam :) I've been having some issues bisecting builds, and was going to pick that up tomorrow, but confirming it's been present a while is at least enough to update the Sec_Impact. Sheriffbot will still nag, but at least it know.

Comment 11 by ricea@chromium.org on Wed, Jan 27, 2021, 11:42 PM EST Project Member

I have a fix, but writing a unit test is going to be challenging.

Comment 12 by ricea@chromium.org on Thu, Jan 28, 2021, 1:18 AM EST Project Member

Cc: yukishiino@chromium.org yhirano@chromium.org

The poc seems to create a really unusual situation where DOMWebSocket is garbage collected without ContextDestroyed() being called but while HasPendingActivity() is still true.

I have two questions:

1. Could this break assumptions and cause issues for classes other than DOMWebSocket?
2. How can I reproduce this state in a unit test? V8TestingScope seems to respect HasPendingActivity(), but then calls ContextDestroyed() when it is destroyed.

I don't know who to ask, so +yukishiino and +yhirano who may be able to identify the right person.

Comment 13 by yukishiino@chromium.org on Thu, Jan 28, 2021, 2:16 AM EST Project Member

I don't fully understand the problem though, it can be a problem of the destruction / sweeping order. In the world of GC, we don't have any guarantee about the destruction / sweeping order.

```
  class Parent : public GCed {
    Member<Child> child_;
  };
```

When the parent object and its |child_| object become unreachable in the same GC cycle, |child_| can be destructed before the parent object gets destructed (= the sweeping order is indeterministic). So, generally speaking, you must not touch any GC object in the destructor.

If you need to do something with GC objects in the destructor, Blink GC supports "prefinalizer" which runs before any object destruction.

I'm not 100% sure, but this could be the cause?

Comment 14 by ricea@chromium.org on Thu, Jan 28, 2021, 2:59 AM EST Project Member

#13 Normally DOMWebSocket::ContextDestroyed is called before the object is destroyed, because otherwise DOMWebSocket::IsPendingActivity will stop the object being collected. However, in this case garbage collection happens while DOMWebSocket::IsPendingActivity is still returning true, even though DOMWebSocket::ContextDestroyed hasn't been called.

DOMWebSocket isn't expecting this and so the use-after-poison arises. I can fix the false assumption in DOMWebSocket that causes the use-after-poison, but I don't know whether other ActiveScriptWrappable classes might be vulnerable. I also haven't found a way to test it automatically.

Comment 15 by yukishiino@chromium.org on Thu, Jan 28, 2021, 3:04 AM EST Project Member

Cc: mlippautz@chromium.org

+cc: mlippautz@ as an expert of ActiveScriptWrappable

Is it guaranteed that an ActiveScriptWrappable object will be destroyed only after ContextDestroyed() is called or only when HasPendingActivity() returns false? Are there any other cases? Pitfalls?

Comment 16 by mlippautz@chromium.org on Thu, Jan 28, 2021, 3:15 AM EST Project Member

> Is it guaranteed that an ActiveScriptWrappable object will be destroyed only after ContextDestroyed() is called or only when HasPendingActivity() returns false? Are there any other cases? Pitfalls?

a) ASW is a regular GCed object that can be held alive via normal references (Persistent, Member);
b) ASW has the HasPendingActivity() mechanism that acts as a conditional root.

Now, for b) is processed the following [1]:
1) If the context is destroyed (we ask ASW itself), then HasPendingActivity() is ignored.
2) Otherwise, we take the result of HasPendingActivity() to decide whether we need to keep ASW alive.
3) Default value for HasPendingActivity() is false.

Pitfalls: None that I know that result in UAF. ASW is generally a problem for keeping the managed heap slim, as it often returns `HasPendingActivity()==true` for a long time which means that we cannot reclaim a lot of memory.

I guess for this particular object it is a problem that it's not notified that the context is destroyed, yet there's a GC that reclaims it (because IsContextDestroed() is already true).

[1]
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/platform/bindings/active_script_wrappable_manager.cc;l=16;drc=dfe9cd6c29a4a1871928ba06c4459305769df2a4;bpv=1;bpt=1?q=ActiveScriptWrappable&ss=chromium

Comment 17 by ricea@chromium.org on Thu, Jan 28, 2021, 3:31 AM EST Project Member

Here's a smaller repro. The call to gc() doesn't seem to be strictly necessary to trigger the crash, but it makes it reliable.

one-page.html
209 bytes View Download

Comment 18 by yhirano@chromium.org on Thu, Jan 28, 2021, 3:34 AM EST Project Member

Is creating two websocket connections necessary?

Comment 19 by mlippautz@chromium.org on Thu, Jan 28, 2021, 3:40 AM EST Project Member

Maybe somebody can chime in on the semantics of observing ContextDestroyed()?

As long as I can remember, all systems (even pre-unified heap) treated context destruction as a signal to reclaim an object. In that sense, receiving ContextDestroyed() before the destructor was never guaranteed. The branch that that overrides HasPendingAcitivity() in the case that the context has been destroyed has been migrated over from object grouping where it has been used for years.

(Changing that override would likely result in a lot of leaks.)

Comment 20 by ricea@chromium.org on Thu, Jan 28, 2021, 3:55 AM EST Project Member

#18 Yes. Removing the second WebSocket creation stops the crash. I have no idea why. Removing the first WebSocket creation also stops the crash.

Comment 21 by ricea@chromium.org on Thu, Jan 28, 2021, 4:48 AM EST Project Member

I managed to reproduce the crash in a unit test by using SetExecutionContext(nullptr). I have a CL in progress at https://chromium-review.googlesource.com/c/chromium/src/+/2655089.

Comment 22 by yhirano@chromium.org on Thu, Jan 28, 2021, 6:05 AM EST Project Member

With DCHECK enabled chrome the reproduction case hits another DCHECK, so I suspect there is a bug around printing and reload.

Comment 23 by bugdroid on Thu, Jan 28, 2021, 6:15 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2dae20b0b3890af23852345a69158c99b47746aa

commit 2dae20b0b3890af23852345a69158c99b47746aa
Author: Adam Rice <ricea@chromium.org>
Date: Thu Jan 28 11:14:43 2021

WebSocket: Don't clear event queue on destruction

It's unnecessary to clear the event queue as it will be garbage
collected anyway. Stop doing it.

Also add a unit test for GC with pending events. This can only happen if
the execution context changes while the events are pending.

~~BUG=1170657~~

Change-Id: I01e5a687587f7471e88640c43f0dfe83e5c01bd1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2655089
Reviewed-by: Yutaka Hirano <yhirano@chromium.org>

Commit-Queue: Adam Rice <ricea@chromium.org>
Cr-Commit-Position: refs/heads/master@{#848065}

[modify] https://crrev.com/2dae20b0b3890af23852345a69158c99b47746aa/third_party/blink/renderer/modules/websockets/dom_websocket_test.cc
[modify] https://crrev.com/2dae20b0b3890af23852345a69158c99b47746aa/third_party/blink/renderer/modules/websockets/dom_websocket.cc

Comment 24 by ricea@chromium.org on Thu, Jan 28, 2021, 6:29 AM EST Project Member

Status: Fixed (was: Started)
NextAction: 2021-01-31

I've fixed the crash with DOMWebSocket; I haven't looked to see if other ActiveScriptWrappables have the same issue.

I plan to request a merge to M89 in two days, assuming the change sticks.

Comment 25 by ricea@chromium.org on Thu, Jan 28, 2021, 7:06 AM EST Project Member

#22 Do you think I should remove that DCHECK? It doesn't seem to be necessary.

Comment 26 by yhirano@chromium.org on Thu, Jan 28, 2021, 7:14 AM EST Project Member

It is at DocumentLoader::BodyDataReceived.

```
DCHECK(data.data());
DCHECK(data.size());
DCHECK(!frame_->GetPage()->Paused());   <<<==========
```

I'm under the impression that the DCHECK is a valid assumption and somebody else breaks that assumption.

Comment 27 by rsleevi@chromium.org on Thu, Jan 28, 2021, 9:30 AM EST Project Member

Cc: adetaylor@chromium.org

Thanks everyone for the fascinating discussion! I appreciate the quick fix in Comment #23, but I'm wanting to make sure that if there's a pattern or class of potential issues, we also take the opportunity to explore those (re: Comment #24 and fixed). Do we have a clear owner who can investigate whether there's something deeper here re: GC and edge conditions? I took Comment #19 as looking for more information, and just wanting to make sure that the Fixed signal doesn't cause this to slip from our radar.

CC'ing adetaylor@ for advice, since I'm not sure whether we'd want to mark this Fixed (for the reported issue), and then spin out another issue to continue investigation/discussion, or if we'd like to use this to continue to drive to a point where we feel we comfortably understand the "why this bug" and have had a chance to make sure we don't have it in other GC'd objects as a pattern (in the event the VRP uses that as a signal when considering this report).

Comment 28 by adetaylor@chromium.org on Thu, Jan 28, 2021, 12:05 PM EST Project Member

Thanks for asking Ryan!

Yeah, the optimal pattern to keep the bots happy is to keep this bug Fixed and raise a new crbug of type=Bug-Security for follow-up work/investigations, so I raised issue 1171790.

Comment 29 by sheriffbot on Thu, Jan 28, 2021, 12:40 PM EST Project Member

Labels: reward-topanel

Comment 30 by sheriffbot on Thu, Jan 28, 2021, 1:55 PM EST Project Member

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

Comment 31 by mlippautz@chromium.org on Thu, Jan 28, 2021, 5:04 PM EST Project Member

In case you want more context on ASW, just add me to 1171790.

Comment 32 by sheriffbot on Fri, Jan 29, 2021, 2:31 PM EST Project Member

Labels: Merge-Request-89

Requesting merge to beta M89 because latest trunk commit (848065) appears to be after beta branch point (843830).

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

Comment 33 by sheriffbot on Fri, Jan 29, 2021, 2:40 PM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89'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), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 34 by adetaylor@chromium.org on Fri, Jan 29, 2021, 3:05 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389.

Comment 35 by bugdroid on Sat, Jan 30, 2021, 1:48 AM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/171d6ee562c3cac850d9705e18745bb1214e5d83

commit 171d6ee562c3cac850d9705e18745bb1214e5d83
Author: Adam Rice <ricea@chromium.org>
Date: Sat Jan 30 06:48:06 2021

WebSocket: Don't clear event queue on destruction

It's unnecessary to clear the event queue as it will be garbage
collected anyway. Stop doing it.

Also add a unit test for GC with pending events. This can only happen if
the execution context changes while the events are pending.

~~BUG=1170657~~

(cherry picked from commit 2dae20b0b3890af23852345a69158c99b47746aa)

Change-Id: I01e5a687587f7471e88640c43f0dfe83e5c01bd1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2655089
Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Commit-Queue: Adam Rice <ricea@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#848065}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2660955
Reviewed-by: Adam Rice <ricea@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#419}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/171d6ee562c3cac850d9705e18745bb1214e5d83/third_party/blink/renderer/modules/websockets/dom_websocket_test.cc
[modify] https://crrev.com/171d6ee562c3cac850d9705e18745bb1214e5d83/third_party/blink/renderer/modules/websockets/dom_websocket.cc

Comment 36 by ricea@chromium.org on Mon, Feb 1, 2021, 1:05 PM EST Project Member

Labels: Merge-Request-88

It looks like this has successfully shipped to beta so requested merge to stable branch M88. I'm on the fence whether this needs a merge, since I have found no way to reproduce without human interaction.

> 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
> * Full automated unit test coverage

Yes!

> * Deployed in Canary for at least 24 hours

Yes!

> * Safe Merge

About as safe as a merge can be. The change just removes some code which was not needed anyway.

> - Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines

N/A

> 2. Links to the CLs you are requesting to merge.

https://chromium-review.googlesource.com/c/chromium/src/+/2660955

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

Yes.

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

Already merged to M89.

> 5. Why are these changes required in this milestone after branch?

Medium-severity security fix.

> 6. Is this a new feature?

No.

> 7. If it is a new feature, is it behind a flag using finch?

N/A

Comment 37 by ricea@chromium.org on Tue, Feb 2, 2021, 3:05 AM EST Project Member

Cc: fergal@chromium.org

+fergal for the question of whether user-triggered reload with the print dialog open should result in loading the page in a paused state.

Comment 38 by fergal@google.com on Tue, Feb 2, 2021, 9:14 PM EST Project Member

That doesn't sound correct to me, if you reload a page (which dismisses the print dialog) then the new page should have no lingering state oddness.

I'm also a bit unclear why you're asking me.

Comment 39 by ricea@chromium.org on Thu, Feb 4, 2021, 4:00 PM EST Project Member

#38 I was informed you were knowledgeable about navigations. Do you know who would be a good person to ask?

Comment 40 by fergal@google.com on Thu, Feb 4, 2021, 5:44 PM EST Project Member

Ah ok, yeah to some extent :) You can ask navigation-dev@. In general we wouldn't load a page paused but whether there are odd exceptions for printing I couldn't say authoritatively.

Comment 41 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:26 PM EST Project Member

Labels: -Merge-Request-88 Merge-Approved-88

Approving merge to M88, branch 4324. Please merge by the end of Thursday PST to get into next Tuesday's release.

Comment 42 by srinivassista@google.com on Thu, Feb 11, 2021, 4:22 PM EST Project Member

Please help complete the merge before friday (Feb 12) - 12pm PST,

Comment 43 by ricea@chromium.org on Thu, Feb 11, 2021, 11:46 PM EST Project Member

Sorry for the delay.

I have a merge CL at https://chromium-review.googlesource.com/c/chromium/src/+/2690730 but the CQ is giving errors which appear unrelated. Should I bypass the CQ?

Comment 44 by bugdroid on Fri, Feb 12, 2021, 5:44 AM EST Project Member

Labels: -merge-approved-88 merge-merged-4324 merge-merged-88

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/b712f9fd66389cf7ebe3145080681995ff25c60f

commit b712f9fd66389cf7ebe3145080681995ff25c60f
Author: Adam Rice <ricea@chromium.org>
Date: Fri Feb 12 10:43:43 2021

WebSocket: Don't clear event queue on destruction

It's unnecessary to clear the event queue as it will be garbage
collected anyway. Stop doing it.

Also add a unit test for GC with pending events. This can only happen if
the execution context changes while the events are pending.

~~BUG=1170657~~

(cherry picked from commit 2dae20b0b3890af23852345a69158c99b47746aa)

(cherry picked from commit 171d6ee562c3cac850d9705e18745bb1214e5d83)

Change-Id: I01e5a687587f7471e88640c43f0dfe83e5c01bd1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2655089
Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Commit-Queue: Adam Rice <ricea@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#848065}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2660955
Reviewed-by: Adam Rice <ricea@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4389@{#419}
Cr-Original-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2690730
Auto-Submit: Adam Rice <ricea@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4324@{#2191}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/b712f9fd66389cf7ebe3145080681995ff25c60f/third_party/blink/renderer/modules/websockets/dom_websocket_test.cc
[modify] https://crrev.com/b712f9fd66389cf7ebe3145080681995ff25c60f/third_party/blink/renderer/modules/websockets/dom_websocket.cc

Comment 45 by adetaylor@google.com on Fri, Feb 12, 2021, 7:35 PM EST Project Member

Labels: Release-3-M88

Comment 46 by achuith@chromium.org on Thu, Feb 18, 2021, 8:53 PM EST Project Member

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

Comment 47 by amyressler@google.com on Mon, Feb 22, 2021, 4:31 PM EST Project Member

Labels: CVE-2021-21157 CVE_description-missing

Comment 48 by amyressler@google.com on Mon, Feb 22, 2021, 4:33 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 49 by gianluca@google.com on Tue, Feb 23, 2021, 4:29 PM EST Project Member

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

Comment 50 by gianluca@google.com on Tue, Feb 23, 2021, 5:17 PM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 51 by achuith@chromium.org on Tue, Feb 23, 2021, 5:31 PM EST Project Member

Labels: -LTS-Merge-Request-86

Comment 52 by bugdroid on Tue, Feb 23, 2021, 6:52 PM EST Project Member

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c57ba0a5dacc78c7a1954c99d381b77ec771fba6

commit c57ba0a5dacc78c7a1954c99d381b77ec771fba6
Author: Adam Rice <ricea@chromium.org>
Date: Tue Feb 23 23:49:23 2021

WebSocket: Don't clear event queue on destruction

It's unnecessary to clear the event queue as it will be garbage
collected anyway. Stop doing it.

Also add a unit test for GC with pending events. This can only happen if
the execution context changes while the events are pending.

~~BUG=1170657~~

(cherry picked from commit 2dae20b0b3890af23852345a69158c99b47746aa)

Change-Id: I01e5a687587f7471e88640c43f0dfe83e5c01bd1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2655089
Reviewed-by: Yutaka Hirano <yhirano@chromium.org>
Commit-Queue: Adam Rice <ricea@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#848065}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2704980
Commit-Queue: Achuith Bhandarkar <achuith@chromium.org>
Reviewed-by: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1548}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/c57ba0a5dacc78c7a1954c99d381b77ec771fba6/third_party/blink/renderer/modules/websockets/dom_websocket.cc

Comment 53 by asumaneev@google.com on Tue, Mar 2, 2021, 10:24 AM EST Project Member

Labels: -LTS-Merge-Approved-86 LTR-Merged-86

Comment 54 by amyressler@google.com on Wed, Mar 3, 2021, 7:34 PM EST Project Member

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

*** Boilerplate reminders! ***
Please do NOT publicly disclose details until a fix has been released to all our users. Early public disclosure may cancel the provisional reward. Also, please be considerate about disclosure when the bug affects a core library that may be used by other products. Please do NOT share this information with third parties who are not directly involved in fixing the bug. Doing so may cancel the provisional reward. Please be honest if you have already disclosed anything publicly or to third parties. Lastly, we understand that some of you are not interested in money. We offer the option to donate your reward to an eligible charity. If you prefer this option, let us know and we will also match your donation - subject to our discretion. Any rewards that are unclaimed after 12 months will be donated to a charity of our choosing.

Please contact security-vrp@chromium.org with any questions.
****

Comment 55 by amyressler@google.com on Wed, Mar 3, 2021, 8:17 PM EST Project Member

Congratulations, neklab2015@! The VRP Panel has decided to award you $5,000 for this report. Nice work!

Comment 56 by amyressler@google.com on Fri, Mar 5, 2021, 11:00 AM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 57 by sheriffbot on Thu, May 6, 2021, 1:51 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 58 by vahl@chromium.org on Thu, Sep 16, 2021, 8:41 AM EDT Project Member

Components: -Blink>MemoryAllocator>GarbageCollection Blink>GarbageCollection