


☆ Starred by 5 users

Owner:

h...@chromium.org

CC:



cindyb@chromium.org

tommi@chromium.org

adetaylor@chromium.org

pbomm...@chromium.org

primiano@chromium.org

achuith@chromium.org

Status:

Verified (Closed)

Components:

Blink>Speech

Modified:

Feb 11, 2021

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

2020-01-15

OS:

Linux, Android, Windows, Chrome, Mac, Fuchsia

Pri:

0

Type:

Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Deadline-Exceeded
Security_Severity-High
allpublic
reward-inprocess
ClusterFuzz-Verified
reward-15000
Test-Predator-Wrong-CLs
Test-Predator-Auto-Components
Test-Predator-Auto-Owner
CVE_description-submitted
Target-79
M-79
VulnerabilityAnalysis-Requested
merge-merged-3945
Merge-Merged-79
merge-merged-3987
merge-merged-80
Release-3-M79
CVE-2020-6378

Issue 1018677: Security: heap-use-after-free in content::SpeechRecognizerImpl::Abort

Reported by [chris...@gmail.com](#) on Mon, Oct 28, 2019, 5:58 AM EDT

 Code

VULNERABILITY DETAILS

heap-use-after-free in content::SpeechRecognizerImpl::Abort

VERSION

Chrome Version: asan-linux-release-709771

REPRODUCTION CASE

`./chrome --headless --screenshot repro.html`

ADDITIONAL INFORMATION

```
[1027/200927.988278:WARNING:ipc_message_attachment_set.cc(49)] MessageAttachmentSet destroyed with unconsumed attachments: 0/1
[1027/200929.719037:INFO:headless_shell.cc(620)] Written to file screenshot.png.
=====
==16970==ERROR: AddressSanitizer: heap-use-after-free on address 0x60b00001bdc8 at pc 0x5555627740c2 bp 0x7ffdf9002c0 sp 0x7ffdf9002b8
READ of size 8 at 0x60b00001bdc8 thread T5 (Chrome_IOThread)
#0 0x5555627740c1 in content::SpeechRecognizerImpl::Abort(blink::mojom::SpeechRecognitionError const&) content/browser/speech/speech_recognizer_impl.cc:750:15
#1 0x555562770f83 in AbortSilently content/browser/speech/speech_recognizer_impl.cc:702:10
#2 0x555562770f83 in content::SpeechRecognizerImpl::ExecuteTransitionAndGetNextState(content::SpeechRecognizerImpl::FSMEventArgs const&)
content/browser/speech/speech_recognizer_impl.cc:369:18
#3 0x55556276d820 in content::SpeechRecognizerImpl::DispatchEvent(content::SpeechRecognizerImpl::FSMEventArgs const&)
content/browser/speech/speech_recognizer_impl.cc:355:12
#4 0x555568057852 in Run base/callback.h:98:12
#5 0x555568057852 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:142:33
#6 0x55556808f8f8 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*, bool*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:365:23
#7 0x55556808f277 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoSomeWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:219:7
#8 0x5555681c7e01 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_libevent.cc:208:55
#9 0x55556809168e in Run base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:463:12
#10 0x55556809168e in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
#11 0x555568008651 in base::RunLoop::Run() base/run_loop.cc:156:14
#12 0x55556146cb04 in content::BrowserProcessSubThread::IOThreadRun(base::RunLoop*) content/browser/browser_process_sub_thread.cc:158:11
#13 0x5555680e126b in base::Thread::ThreadMain() base/threading/thread.cc:376:3
#14 0x5555681ba7b1 in base::(anonymous namespace)::ThreadFunc(void*) base/threading/platform_thread_posix.cc:81:13
#15 0x7ff7f9b96da in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76da)

0x60b00001bdc8 is located 8 bytes inside of 112-byte region [0x60b00001bdc0,0x60b00001be30)
freed by thread T5 (Chrome_IOThread) here:
#0 0x555565c5f36d in operator delete(void*) /b/warming/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
#1 0x555568057852 in Run base/callback.h:98:12
#2 0x555568057852 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:142:33
#3 0x55556808f8f8 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*, bool*)
```

```
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:365:23
#4 0x5556808f277 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoSomeWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:219:7
#5 0x555681c7e01 in base::MessagePumpLibevent::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_libevent.cc:208:55
#6 0x5556809168e in Run base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:463:12
#7 0x5556809168e in non-virtual thunk to base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run(bool, base::TimeDelta)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc
#8 0x55568008651 in base::RunLoop::Run() base/run_loop.cc:156:14
#9 0x5556146cb4 in content::BrowserProcessSubThread::IOThreadRun(base::RunLoop*) content/browser/browser_process_sub_thread.cc:158:11
#10 0x555680e126b in base::Thread::ThreadMain() base/threading/thread.cc:376:3
#11 0x555681ba7b1 in base::(anonymous namespace)::ThreadFunc(void*) base/threading/platform_thread_posix.cc:81:13
#12 0x7ffff9b96da in start_thread (/lib/x86_64-linux-gnu/libpthread.so.0+0x76da)

previously allocated by thread T0 (chrome) here:
#0 0x5555e5ceb0d in operator new(unsigned long) /b/swarming/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
#1 0x55556144dadd in content::BrowserMainLoop::BrowserThreadsStarted() content/browser/browser_main_loop.cc:1384:39
#2 0x55562421694 in Run base/callback.h:98:12
#3 0x55562421694 in content::StartupTaskRunner::RunAllTasksNow() content/browser/startup_task_runner.cc:41:29
#4 0x5556144bc41 in content::BrowserMainLoop::CreateStartupTasks() content/browser/browser_main_loop.cc:917:25
#5 0x555614548ad in content::BrowserMainRunnerImpl::Initialize(content::MainFunctionParams const&) content/browser/browser_main_runner_impl.cc:128:15
#6 0x5557907b11 in headless::HeadlessContentMainDelegate::RunProcess(std::::__1::basic_string<char, std::::__1::char_traits<char>, std::::__1::allocator<char>> const&, content::MainFunctionParams const&) headless/lib/headless_content_main_delegate.cc:318:35
#7 0x555670821fd in RunBrowserProcessMain content/app/content_main_runner_impl.cc:524:29
#8 0x555670821fd in content::ContentMainRunnerImpl::RunServiceManager(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:960:10
#9 0x55567081703 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:868:12
#10 0x5556722201f in service_manager::Main(service_manager::MainParams const&) services/service_manager/embedder/main.cc:423:29
#11 0x5556707ca3f in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:19:10
#12 0x5556721d7ef in headless::(anonymous namespace)::RunContentMain(headless::HeadlessBrowser::Options, base::OnceCallback<void (headless::HeadlessBrowser*)>)> headless/app/headless_shell.cc:172:10
#13 0x5556721c7e6 in HeadlessBrowserMain headless/app/headless_shell.cc:861:10
#14 0x5556721c7e6 in headless::HeadlessShellMain(int, char const**) headless/app/headless_shell.cc:806:10
#15 0x5555e5d1618 in ChromeMain chrome/app/chrome_main.cc:106:12
#16 0x7ffff06efb96 in __libc_start_main /build/glibc-OTSdL5/glibc-2.27/csu/./csu/libc-start.c:310
```

```
Thread T5 (Chrome_IOThread) created by T0 (chrome) here:
#0 0x5555e58fcca in pthread_create /b/swarming/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_interceptors.cpp:214:3
#1 0x555681b99fe in base::(anonymous namespace)::CreateThread(unsigned long, bool, base::PlatformThread::Delegate*, base::PlatformThreadHandle*, base::ThreadPriority) base/threading/platform_thread_posix.cc:120:13
#2 0x555680e04e4 in base::Thread::StartWithOptions(base::Thread::Options const&) base/threading/thread.cc:182:15
#3 0x555621a1842 in content::BrowserTaskExecutor::CreateIOThread() content/browser/scheduler/browser_task_executor.cc:341:19
#4 0x55567081d7c in content::ContentMainRunnerImpl::RunServiceManager(content::MainFunctionParams&, bool) content/app/content_main_runner_impl.cc:937:9
#5 0x55567081703 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:868:12
#6 0x5556722201f in service_manager::Main(service_manager::MainParams const&) services/service_manager/embedder/main.cc:423:29
#7 0x5556707ca3f in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:19:10
#8 0x5556721d7ef in headless::(anonymous namespace)::RunContentMain(headless::HeadlessBrowser::Options, base::OnceCallback<void (headless::HeadlessBrowser*)>)> headless/app/headless_shell.cc:172:10
#9 0x5556721c7e6 in HeadlessBrowserMain headless/app/headless_shell.cc:861:10
#10 0x5556721c7e6 in headless::HeadlessShellMain(int, char const**) headless/app/headless_shell.cc:806:10
#11 0x5555e5d1618 in ChromeMain chrome/app/chrome_main.cc:106:12
#12 0x7ffff06efb96 in __libc_start_main /build/glibc-OTSdL5/glibc-2.27/csu/./csu/libc-start.c:310
```

SUMMARY: AddressSanitizer: heap-use-after-free content/browser/speech/speech_recognizer_impl.cc:750:15 in content::SpeechRecognizerImpl::Abort(blink::mojom::SpeechRecognitionError const&)

Shadow bytes around the buggy address:

```
0x0c167ffb760: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa
0x0c167ffb770: fa fa fa fa fa fa 00 00 00 00 00 00 00 00 00 00
0x0c167ffb780: 00 00 00 fa fa fa fa fa fa fa fa 00 00 00 00
0x0c167ffb790: 00 00 00 00 00 00 00 00 00 fa fa fa fa fa fa
0x0c167ffb7a0: fa fa 00 00 00 00 00 00 00 00 00 00 00 00 00 fa
=>0x0c167ffb7b0: fa fa fa fa fa fa fd[fd]fd fd fd fd fd fd
0x0c167ffb7c0: fd fd fd fd fd fd fa fa fa fa fa fa 00 00
0x0c167ffb7d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 fa fa fa
0x0c167ffb7e0: fa fa fa fa fd fd fd fd fd fd fd fd fd fd
0x0c167ffb7f0: fd fa fa fa fa fa fa fa fa fd fd fd fd fd fd
0x0c167ffb800: fd fd fd fd fd fd fa fa fa fa fa fa fa fa
```

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
==16970==ABORTING
```

CREDIT INFORMATION

Antti Levomäki and Christian Jalio from Forcepoint

[repro.html](#)
118 KB [View](#) [Download](#)

[Comment 1](#) Deleted

[Comment 2](#) Deleted

[Comment 3](#) by ClusterFuzz on Mon, Oct 28, 2019, 12:32 PM EDT
ClusterFuzz is analyzing your testcase. Developers can follow the progress at <https://clusterfuzz.com/testcase?key=6008750152220672>.

[Comment 4](#) by ClusterFuzz on Mon, Oct 28, 2019, 4:03 PM EDT

Labels: Test-Predator-Auto-Components
Components: Blink>Speech

Automatically applying components based on crash stacktrace and information from OWNERS files.

If this is incorrect, please apply the Test-Predator-Wrong-Components label.

[Comment 5](#) by [ClusterFuzz](#) on Mon, Oct 28, 2019, 4:03 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: olivierrobin@chromium.org
Labels: Test-Predator-Auto-Owner

Automatically assigning owner based on suspected regression changelist
<https://chromium.googlesource.com/chromium/src/+9109135db0b25604af35c2031f41a61816584b0a> ([EG2] Converts SaveProfileEGTest).

If this is incorrect, please let us know why and apply the Test-Predator-Wrong-CLs label. If you aren't the correct owner for this issue, please unassign yourself as soon as possible so it can be re-triaged.

[Comment 6](#) by [ClusterFuzz](#) on Mon, Oct 28, 2019, 4:03 PM EDT

Labels: Security_Impact-Stable Security_Severity-Critical

Detailed Report: <https://clusterfuzz.com/testcase?key=6008750152220672>

Fuzzer:

Job Type: linux_asan_chrome_mp

Platform Id: linux

Crash Type: Heap-use-after-free READ 8

Crash Address: 0x60f0000171e8

Crash State:

content::SpeechRecognizerImpl::Abort
content::SpeechRecognizerImpl::ExecuteTransitionAndGetNextState
content::SpeechRecognizerImpl::DispatchEvent

Sanitizer: address (ASAN)

Recommended Security Severity: Critical

Regressed: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=709912:709913

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=6008750152220672

The reproduce tool requires a ClusterFuzz source checkout. To prepare one, run:

git clone <https://github.com/google/clusterfuzz> && cd clusterfuzz && git checkout tags/reproduce-tool-stable

To reproduce this issue, run:

./reproduce.sh -t <https://clusterfuzz.com/testcase-detail/6008750152220672> -b /path/to/build

Please use the GN arguments provided in this report when building the binary. If you have any feedback on reproducing test cases, let us know at <https://forms.gle/Yh3qCYFvHj6E5jz5> so we can improve.

A recommended severity was added to this bug. Please change the severity if it is inaccurate.

[Comment 7](#) by [olivierrobin@chromium.org](#) on Mon, Oct 28, 2019, 4:07 PM EDT

Status: Untriaged (was: Assigned)
Owner: ----
Labels: Test-Predator-Wrong-CLs OS-Linux

My CL is iOS only.

[Comment 8](#) by [jdeblasio@chromium.org](#) on Mon, Oct 28, 2019, 4:50 PM EDT

Status: Assigned (was: Untriaged)
Owner: tommy@chromium.org
Labels: -Security_Severity-Critical Security_Severity-High Pri-1

tommy@: can you take a look at this as the speech synth owner and help us triage it? It appears to trigger a crash of some kind in Chrome since roughly the beginning of time, so I can't easily bisect it further.

I'm dropping this to High given the required command line flags. Frankly, even that might be a stretch, but until we understand what's happening, better safe than sorry.

[Comment 9](#) by [jdeblasio@chromium.org](#) on Mon, Oct 28, 2019, 4:50 PM EDT

Labels: M-78

[Comment 10](#) by [tommy@chromium.org](#) on Mon, Oct 28, 2019, 5:38 PM EDT

Owner: myid...@igalia.com
Cc: tommy@chromium.org

myid.shin - could this be related to the recent Mojo changes?
(e.g. here: <https://chromium-review.googlesource.com/c/chromium/src/+1872090>)

[Comment 11](#) by [myid...@igalia.com](#) on Mon, Oct 28, 2019, 11:19 PM EDT

Status: Available (was: Assigned)
Owner: ----

Hi, tommy@,

I don't think Mojo changes are related to this issue since the CL only converted the old Mojo to the new one and it doesn't change any work flow.
And I've also reproduced this issue with reverting the CL.

BTW, I I took a look at this issue(I didn't do a bisect for this).

UAF issue is caused by accessing listener, SpeechRecognitionEventListener(=SpeechRecognitionManagerImpl) after destroying SpeechRecognitionManagerImpl.

SpeechRecognizerImpl::AbortRecognition --> Post to IO thread
BrowserMainLoop shutdown and SpeechRecognitionManagerImpl is nullptr
SpeechRecognizerImpl::Abort -> Access SpeechRecognitionManagerImpl and crash.

So, I could see to stop the reproduction if we use a weak pointer instead of [this] in SpeechRecognizerImpl::AbortRecognition.

```
void SpeechRecognizerImpl::AbortRecognition() {  
  base::PostTask(FROM_HERE, {BrowserThread::IO},
```

```
base::BindOnce(&SpeechRecognizerImpl::DispatchEvent, weak_ptr_factory_.GetWeakPtr()) /*instead of this*/,
FSMEventArgs(EVENT_ABORT));
}
```

I think we might need a bisect given that this code was added a long time ago and that this issue has recently occurred. WDYT?

[Comment 12](#) by tommi@chromium.org on Tue, Oct 29, 2019, 4:44 AM EDT

Owner: h...@chromium.org

Hans - this vaguely rings a bell - is this a duplicate of a previous issue in SpeechRecognizerImpl?

[Comment 13](#) by sheriffbot@chromium.org on Tue, Oct 29, 2019, 11:16 AM EDT

Status: Assigned (was: Available)

[Comment 14](#) by h...@chromium.org on Tue, Nov 5, 2019, 4:01 AM EST

Cc: primiano@chromium.org

+primiano

> Hans - this vaguely rings a bell - is this a duplicate of a previous issue in SpeechRecognizerImpl?

It doesn't ring a bell for me (but my memory of all this is fading), and I don't find anything in the bug tracker.

myid.shin, your solution sounds plausible. Want to send out a CL and cc myself and primiano?

[Comment 15](#) by sheriffbot@chromium.org on Tue, Nov 19, 2019, 9:10 AM EST

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

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

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

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

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

[Comment 16](#) by sheriffbot@chromium.org on Wed, Dec 4, 2019, 9:10 AM EST

hans: Uh oh! This issue still open and hasn't been updated in the last 29 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

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

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

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

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

[Comment 17](#) by sheriffbot@chromium.org on Wed, Dec 11, 2019, 9:11 AM EST

Labels: -M-78 Target-79 M-79

[Comment 18](#) by sheriffbot@chromium.org on Fri, Dec 27, 2019, 10:41 AM EST

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 19](#) by h...@chromium.org on Tue, Jan 7, 2020, 7:39 AM EST

Status: Started (was: Assigned)

I'm not sure how I ended up owning this, but here's a patch anyway :-)

Patch: <https://chromium-review.googlesource.com/c/chromium/src/+1989069>

[Comment 20](#) by bugdroid on Thu, Jan 9, 2020, 5:53 AM EST

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+57f988dd7c1f63f59b44282efcc9e6f1e85ac19c>

commit [57f988dd7c1f63f59b44282efcc9e6f1e85ac19c](https://chromium.googlesource.com/chromium/src.git/+57f988dd7c1f63f59b44282efcc9e6f1e85ac19c)

Author: Hans Wennborg <hans@chromium.org>

Date: Thu Jan 09 10:52:37 2020

Use a WeakPtr in SpeechRecognizerImpl::AbortRecognition

It seems that during shutdown, the object can go away before the posted task runs.

Thanks to Miyoung Shin for looking into this.

[Bug: 10318677](#)

Change-Id: [11b3c7947eb3110ae6538249106a87f5c56f6238c](https://chromium-review.googlesource.com/c/chromium/src/+1989069)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1989069>

Reviewed-by: Primiano Tucci <primiano@chromium.org>

Reviewed-by: Tommi <tommi@chromium.org>

Reviewed-by: Olga Sharonova <olka@chromium.org>

Commit-Queue: Olga Sharonova <olka@chromium.org>

Cr-Commit-Position: refs/heads/master@{#729694}

[modify] https://crrev.com/57f988dd7c1f63f59b44282efcc9e6f1e85ac19c/content/browser/speech/speech_recognizer_impl.cc

[Comment 21](#) by h...@chromium.org on Thu, Jan 9, 2020, 8:11 AM EST

Status: Fixed (was: Started)

[Comment 22](#) by sheriffbot@chromium.org on Thu, Jan 9, 2020, 10:43 AM EST

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

[Comment 23](#) by sheriffbot@chromium.org on Thu, Jan 9, 2020, 11:03 AM EST

Labels: Merge-Request-80 Merge-Request-79

Requesting merge to stable M79 because latest trunk commit (729694) appears to be after stable branch point (706915).

Requesting merge to beta M80 because latest trunk commit (729694) appears to be after beta branch point (722274).

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

Comment 24 by ClusterFuzz on Thu, Jan 9, 2020, 2:17 PM EST

Status: Verified (was: Fixed)

Labels: ClusterFuzz-Verified

ClusterFuzz testcase 6008750152220672 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=727557:727558

If this is incorrect, please add the ClusterFuzz-Wrong label and re-open the issue.

Comment 25 by sheriffbot@chromium.org on Fri, Jan 10, 2020, 5:56 AM EST

Labels: -Merge-Request-80 Merge-Review-80 Hotlist-Merge-Review

This bug requires manual review: M80'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://goto.google.com/chrome-release-branch-merge-guidelines>
- 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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: govind@ (Android), Kariahda@ (iOS), dgagnon@ (ChromeOS), srinivassista@ (Desktop)

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

Comment 26 by h...@chromium.org on Fri, Jan 10, 2020, 6:39 AM EST

I'm not sure this is severe enough to consider merging, but I'll leave that decision to others.

Comment 27 by srinivassista@google.com on Fri, Jan 10, 2020, 12:45 PM EST

Cc: adetaylor@chromium.org

adetaylor@ can u review if this needs to be merged to M80

Comment 28 Deleted

Comment 29 by srinivassista@google.com on Fri, Jan 10, 2020, 4:59 PM EST

Labels: -Merge-Review-80 Merge-Approved-80

Merge approved for M80, branch:3987

Comment 30 by sheriffbot@chromium.org on Sat, Jan 11, 2020, 10:19 AM EST

Labels: -Pri-1 Pri-0

Setting Pri-0 to match security severity Critical. 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 31 by gov...@chromium.org on Mon, Jan 13, 2020, 2:58 AM EST

Cc: pbomm...@chromium.org

How is the change looking in canary so far?

Comment 32 by h...@chromium.org on Mon, Jan 13, 2020, 9:03 AM EST

> How is the change looking in canary so far?

I haven't heard anything, so I assume it's good.

Comment 33 by srinivassista@google.com on Mon, Jan 13, 2020, 1:55 PM EST

Please help get your merges complete before 3pm PST today Monday Jan 13 so this can be included in the beta release tomorrow

Comment 34 by gov...@google.com on Mon, Jan 13, 2020, 2:23 PM EST

M80 merge going thru CQ - <https://chromium-review.googlesource.com/c/chromium/src/+1998316>.

Comment 35 by bugdroid on Mon, Jan 13, 2020, 4:28 PM EST

Labels: -merge-approved-80 merge-merged-3987 merge-merged-80

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+0875eb6ea4bf56bd54f01097116451fa0f66d138>

commit 0875eb6ea4bf56bd54f01097116451fa0f66d138

Author: Hans Wennborg <hans@chromium.org>

Date: Mon Jan 13 21:27:26 2020

Use a WeakPtr in SpeechRecognizerImpl::AbortRecognition

It seems that during shutdown, the object can go away before the posted task runs.

Thanks to Miyoung Shin for looking into this.

(cherry picked from commit 57f988dd7c1f63f59b44282efcc9e6f1e85ac19c)

Bug-1018677

Change-Id: I1b3c7947eb3110ae6538249106a87f5c56f6238c

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1989069>

Reviewed-by: Primiano Tucci <primiano@chromium.org>

Reviewed-by: Tommi <tonmi@chromium.org>

Reviewed-by: Olga Sharonova <olka@chromium.org>

Commit-Queue: Olga Sharonova <olka@chromium.org>

Cr-Original-Commit-Position: refs/heads/master@{#729694}

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1998316>

Reviewed-by: Krishna Govind <govind@chromium.org>

Reviewed-by: Hans Wennborg <hans@chromium.org>
Commit-Queue: Hans Wennborg <hans@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#497}
Cr-Branched-From: [c4e8da9871cc266be74481e212f3a5252972509d](https://crrev.com/0875eb6ea4bf56bd54f01097116451fa0f6d138/content/browser/speech/speech_recognizer_impl.cc)-refs/heads/master@{#722274}

[modify] https://crrev.com/0875eb6ea4bf56bd54f01097116451fa0f6d138/content/browser/speech/speech_recognizer_impl.cc

[Comment 36](#) by gov...@google.com on Mon, Jan 13, 2020, 4:34 PM EST

Test failure reported - <https://chromium-review.googlesource.com/c/chromium/src/+1998316>.

Try jobs failed on following builders:

luci.chromium.try-beta/linux-chromeos-rel JOB_FAILED <https://ci.chromium.org/b/8891351525448987248>
1 Test Suite(s) failed.

****non_viz_content_browsertests**** failed because of:

- WithoutCORBProtectionSniffing/CrossSiteDocumentBlockingTest.AppCache_NetworkFallback/0

Is it ok to have merge listed at #35 with above test failure in M80?

[Comment 37](#) by natashapabral@google.com on Tue, Jan 14, 2020, 11:56 AM EST

Labels: reward-topanel

[Comment 38](#) by mmoroz@chromium.org on Tue, Jan 14, 2020, 1:25 PM EST

Labels: VulnerabilityAnalysis-Requested

[hans@](#), thank you for fixing this issue. Chrome Security team needs your knowledge to prevent that whole class of bugs from happening elsewhere. We would greatly appreciate if you could tell us more about the issue by filling out the following form: <https://forms.gle/VWKDUv9a8GXCCRWm7>

[Comment 39](#) by gov...@chromium.org on Tue, Jan 14, 2020, 1:41 PM EST

NextAction: 2020-01-15

Please update bug with M80 Beta result tomorrow morning so we can approve merge to M79 for respin this week.

[Comment 40](#) by gov...@chromium.org on Tue, Jan 14, 2020, 1:56 PM EST

Cc: cindyb@chromium.org

+cindyb@ (Chrome OS M79 Release TPM)

[Comment 41](#) by adetaylor@google.com on Tue, Jan 14, 2020, 3:35 PM EST

[govind@](#) regarding [#c36](#), as far as I can see, the test failure is completely unrelated to the fix here, so it should be safe. I assume it's just a flakey test. It would be good to hear from [hans@](#) as well though for a second opinion.

[Comment 42](#) by gov...@chromium.org on Wed, Jan 15, 2020, 1:03 AM EST

Thank you [adetaylor@](#).

[hans@](#), ptal [comment #41](#) and reply please. Also how is the change looking in Desktop Beta version 80.0.3987.53 which went out this morning?

Note: We would like to cut M79 stable RC tomorrow, Wednesday morning .

[Comment 43](#) by h...@chromium.org on Wed, Jan 15, 2020, 3:04 AM EST

> ptal [comment #41](#) and reply please

The test failure was on a tryjob on linux-chromeos-rel. The test is unrelated, and the second run on that trybot came back green, so that was just an unrelated test being flaky.

> Also how is the change looking in Desktop Beta version 80.0.3987.53 which went out this morning?

I haven't heard about any problems, so I assume it's fine.

[Comment 44](#) by gov...@chromium.org on Wed, Jan 15, 2020, 3:09 AM EST

Labels: -Merge-Request-79 Merge-Approved-79

Thank you [hans@](#).

Approving merge to M79 branch 3945 based on comments [#41](#) and [#43](#). Please merge by EOD today (Munich time) if change continue to look good in canary.

[Comment 45](#) by h...@chromium.org on Wed, Jan 15, 2020, 3:11 AM EST

> Please merge by EOD today (Munich time) if change continue to look good in canary.

I don't know how to merge. Am I supposed to do this myself and are there instructions somewhere? The M80 merge was done by you I think?

[Comment 46](#) by gov...@chromium.org on Wed, Jan 15, 2020, 3:19 AM EST

Ah,ok.

Here is M79 merge - <https://chromium-review.googlesource.com/c/chromium/src/+2001728>. Please review and trigger CQ when ready.

[Comment 47](#) by bugdroid on Wed, Jan 15, 2020, 3:23 AM EST

Labels: -merge-approved-79 merge-merged-79 merge-merged-3945

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+ba6d9c9556a4bb53a825edd481a41cc8aa63a3d3>

commit [ba6d9c9556a4bb53a825edd481a41cc8aa63a3d3](https://chromium.googlesource.com/chromium/src.git/+ba6d9c9556a4bb53a825edd481a41cc8aa63a3d3)

Author: Hans Wennborg <hans@chromium.org>

Date: Wed Jan 15 08:22:02 2020

Use a WeakPtr in SpeechRecognizerImpl::AbortRecognition

It seems that during shutdown, the object can go away before the posted task runs.

Thanks to Miyoung Shin for looking into this.

TBR=olka

(cherry picked from commit [57f988dd7c1f63f59b44282efcc9e6f1e85ac19c](https://chromium-review.googlesource.com/c/chromium/src/+1989069))

~~[Bug-1019677](#)~~

Change-Id: [11b3c7947eb3110ae6538249106a87f5c56f6238c](https://chromium-review.googlesource.com/c/chromium/src/+1989069)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1989069>

Reviewed-by: Primiano Tucci <primiano@chromium.org>
Reviewed-by: Tommi <tommi@chromium.org>
Reviewed-by: Olga Sharonova <olka@chromium.org>
Commit-Queue: Olga Sharonova <olka@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#729694}
Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2001728>
Reviewed-by: Hans Wennborg <hans@chromium.org>
Commit-Queue: Hans Wennborg <hans@chromium.org>
Cr-Commit-Position: refs/branch-heads/3945@{#1043}
Cr-Branch-From: e4635ff7defbae0f9c29e798349f6c0cce4b1b-refs/heads/master@{#706915}

[modify] https://crrev.com/ba6d9c9556a4bb53a825edd481a41cc8aa63a3d3/content/browser/speech/speech_recognizer_impl.cc

[Comment 48](#) by adetaylor@google.com on Wed, Jan 15, 2020, 5:47 PM EST
Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

[Comment 49](#) by adetaylor@google.com on Wed, Jan 15, 2020, 5:47 PM EST
Labels: Release-3-M79

[Comment 50](#) by adetaylor@chromium.org on Wed, Jan 15, 2020, 5:59 PM EST
Labels: CVE-2020-6378 CVE_description-missing

[Comment 51](#) by adetaylor@google.com on Wed, Jan 15, 2020, 7:59 PM EST
Deleted [#c28](#) since I said something daft. The rest of the comment said:

> Yes, this definitely needs to go back to M80 and into the next M79 release.
> This is a use-after-free within the browser process which is triggered by untrustworthy internet content (https://clusterfuzz.com/viewer?testcase_id=6008750152220672&key=7ef832a7-91f0-4cde-bfb0-9fb3602e3c22) so this definitely qualifies as 'critical' severity. Such bugs are rare.

and I bumped the severity up to Critical.

[Comment 52](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 4:21 PM EST
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 53](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 4:25 PM EST
Congrats the Panel decided to reward \$5,000 for this report!

[Comment 54](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 4:28 PM EST
Labels: -Security_Severity-Critical Security_Severity-High

[Comment 55](#) by natashapabrai@google.com on Thu, Jan 23, 2020, 5:05 PM EST
Labels: -reward-unpaid reward-inprocess

[Comment 56](#) by adetaylor@chromium.org on Mon, Feb 10, 2020, 4:35 PM EST
Labels: -CVE_description-missing CVE_description-submitted

[Comment 57](#) by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST
Cc: achuith@chromium.org

[Comment 58](#) by sheriffbot on Sat, Apr 18, 2020, 2:57 PM EDT
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 59](#) by adetaylor@google.com on Wed, Dec 16, 2020, 7:10 PM EST
Labels: -reward-5000 reward-15000

The VRP panel has reconsidered this bug and decided to award \$15,000 in total (so \$10,000 more).

[Comment 60](#) by adetaylor@google.com on Mon, Feb 8, 2021, 11:03 AM EST
Labels: -reward-inprocess reward-unpaid

[Comment 61](#) by amyressler@google.com on Thu, Feb 11, 2021, 4:13 PM EST
Labels: -reward-unpaid reward-inprocess