☆ Starred by 1 user

Owner:	dmazz...@chromium.org
CC:	tommi@chromium.org gshires@chromium.org rockot@google.com oksamyt@chromium.org achuith@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Mojo Internals>SpeechSynthesis
Modified:	May 15, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

reward-5000
Security_Impact-Stable
Arch-x86_64
M-80
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
Target-79
Target-80
VulnerabilityAnalysis-Requested
merge-merged-3987
merge-merged-80
merge-merged-4044
merge-merged-81
Release-2-M80
CVE-2020-6386

Issue 1043603: use-after-poison in mojo::MessageDispatcher

Reported by cdsrc...@gmail.com on Mon, Jan 20, 2020, 5:12 AM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.117 Safari/537.36

Steps to reproduce the problem:
1.build chrome with asan.(Chromium 81.0.4016.0)
2.chrome ./main.html
3.click play button.

Repro uap immediately or occasionally get oom. If oom happens, try again.

What is the expected behavior?

What went wrong?

```
==5094==ERROR: AddressSanitizer: use-after-poison on address 0x7e86da2c4570 at pc 0x5598ad0269a5 bp 0x7ffc063c3350 sp 0x7ffc063c3348
READ of size 8 at 0x7e86da2c4570 thread T0 (chrome)
    #0 0x5598ad0269a4 in mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*) mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:554:54
    #1 0x5598ad032e72 in mojo::MessageDispatcher::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/message_dispatcher.cc:41:19
    #2 0x5598ad03d48b in mojo::internal::MultiplexRouter::ProcessIncomingMessage(mojo::internal::MultiplexRouter::MessageWrapper*,
mojo::internal::MultiplexRouter::ClientCallBehavior, base::SequencedTaskRunner*) mojo/public/cpp/bindings/lib/multiplex_router.cc:883:42
    #3 0x5598ad03bbbe in mojo::internal::MultiplexRouter::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/multiplex_router.cc:604:38
    #4 0x5598ad032e72 in mojo::MessageDispatcher::Accept(mojo::Message*) mojo/public/cpp/bindings/lib/message_dispatcher.cc:41:19
    #5 0x5598ad01be8a in mojo::Connector::DispatchMessage(mojo::Message) mojo/public/cpp/bindings/lib/connector.cc:539:49
    #6 0x5598ad01e052 in mojo::Connector::ReadAllAvailableMessages() mojo/public/cpp/bindings/lib/connector.cc:627:12
    #7 0x5598ad086bdd in Run base/callback.h:132:12
    #8 0x5598ad086bdd in mojo::SimpleWatcher::OnHandleReady(int, unsigned int, mojo::HandleSignalsState const&) mojo/public/cpp/system/simple_watcher.cc:292:14
    #9 0x5598acb99b5e in Run base/callback.h:98:12
    #10 0x5598acb99b5e in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:142:33
    #11 0x5598acbd3659 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
    #12 0x5598acbd2fc2 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoSomeWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:219:7
    #13 0x5598acad5dc0 in base::MessagePumpDefault::Run(base::MessagePump::Delegate*) base/message_loop/message_pump_default.cc:39:55
    #14 0x5598acbd54a4 in Run base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:463:12
    #15 0x5598acbd54a4 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
    #16 0x5598acb4774d in base::RunLoop::Run() base/run_loop.cc:155:14
    #17 0x5598be041b0b in content::RendererMain(content::MainFunctionParams const&) content/renderer/renderer_main.cc:213:16
    #18 0x5598abae9796 in content::ContentMainRunnerImpl::Run(bool) content/app/content_main_runner_impl.cc:880:10
    #19 0x5598abc93c67 in service_manager::Main(service_manager::MainParams const&) services/service_manager/embedder/main.cc:423:29
    #20 0x5598abae4846 in content::ContentMain(content::ContentMainParams const&) content/app/content_main.cc:19:10
    #21 0x5598a2abd03f in ChromeMain chrome/app/chrome_main.cc:121:12
    #22 0x7f72482fab96 in __libc_start_main /build/glibc-OTsEL5/glibc-2.27/csu/../csu/libc-start.c:310

Address 0x7e86da2c4570 is a wild pointer.
SUMMARY: AddressSanitizer: use-after-poison mojo/public/cpp/bindings/lib/interface_endpoint_client.cc:554:54 in
```

```
mojo::InterfaceEndpointClient::HandleValidatedMessage(mojo::Message*)
Shadow bytes around the buggy address:
  0x0fd15b450850: f7 f7 f7 f7 f7 f7 06 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd15b450860: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 06 f7 f7 f7 f7 f7
  0x0fd15b450870: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd15b450880: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 06 00 00
  0x0fd15b450890: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
=>0x0fd15b4508a0: 00 06 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7[f7]f7
  0x0fd15b4508b0: f7 f7 f7 f7 f7 06 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd15b4508c0: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x0fd15b4508d0: f7 f7 f7 f7 f7 f7 f7 f7 f7 06 00 00 00 00 00 00
  0x0fd15b4508e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
  0x0fd15b4508f0: 00 00 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
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
==5094==ABORTING
```

Did this work before? N/A

Chrome version: Chromium 81.0.4016.0   Channel: n/a
OS Version: 18.04
Flash Version:

[Deleted] **main.html**

[Deleted] **poc.html**

Comment 1 by ClusterFuzz on Tue, Jan 21, 2020, 4:18 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5009276533800960.

Comment 2 by ClusterFuzz on Tue, Jan 21, 2020, 4:53 PM EST Project Member

Labels: Security_Impact-Stable

Testcase 5009276533800960 failed to reproduce the crash. Please inspect the program output at https://clusterfuzz.com/testcase?key=5009276533800960.

Comment 3 by est...@chromium.org on Tue, Jan 21, 2020, 6:04 PM EST Project Member

Owner: dmazz...@chromium.org
Cc: tommi@chromium.org gshires@chromium.org oksamyt@chromium.org rockot@google.com
Components: Internals>Mojo Internals>SpeechSynthesis

I'm unable to reproduce this on Linux. Reporter: have you tested on Linux as well or just Windows?

I'm not sure if this would be a SpeechSynthesisUtterance bug or a Mojo bug, so adding some owners of both. Please take a look and see if you have any idea what might be going on? Thanks!

Comment 4 by cdsrc...@gmail.com on Tue, Jan 21, 2020, 11:17 PM EST

I have tested 2 versions of chrome(79.0.3945.130 Release build 64bit, 81.0.4035.0 Dev build 64 bit) in Windows and both can be reproduced.
Attached is the original POC, which may reproduce more steadily.

original_poc.zip
1.1 KB Download

Comment 5 by ClusterFuzz on Tue, Jan 21, 2020, 11:45 PM EST Project Member

ClusterFuzz is analyzing your testcase. Developers can follow the progress at https://clusterfuzz.com/testcase?key=5653134376501248.

Comment 6 by ClusterFuzz on Wed, Jan 22, 2020, 12:18 AM EST Project Member

Testcase 5653134376501248 failed to reproduce the crash. Please inspect the program output at https://clusterfuzz.com/testcase?key=5653134376501248.

Comment 7 by sheriffbot@chromium.org on Wed, Jan 22, 2020, 1:01 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Comment 8 by est...@chromium.org on Wed, Jan 22, 2020, 6:59 PM EST Project Member

Labels: Needs-Feedback

We've still failed to reproduce this on a Windows asan build. Reporter, are you in a fresh profile? Do you have any extensions installed or unusual flags flipped?

Comment 9 by cdsrc...@gmail.com on Thu, Jan 23, 2020, 8:11 AM EST

I did not use any extensions or unusual flags,just fresh profile.
The attachment is a new POC. I have tested it on both real and virtual machines, and it can reproduce more stably.
Can you try this?
Test Env.
Chrome Version 81.0.4023.0 (Developer Build) (64-bit)
OS:Ubuntu 18.04

repro step:
1.python3.6m -m http.server 8605
2./chrome --user-data-dir=/tmp/8888 --incognito http://127.0.0.1:8605/main.html
3.click "play" button.

poc3.zip
700 bytes Download

Comment 10 by est...@chromium.org on Mon, Jan 27, 2020, 2:34 PM EST Project Member

Labels: -Needs-Feedback Security_Severity-High

Ah, great, c9 works for me on Linux. Thank you so much for the repro!

SpeechSynthesizer/Mojo folks, could you please take a look? See repro in comment #9 which works for me on an ASAN build from ToT.

Comment 11 by oksamyt@chromium.org on Mon, Jan 27, 2020, 5:41 PM EST Project Member

Will discuss it in Mojo triage tomorrow.

Comment 12 by sheriffbot@chromium.org on Tue, Jan 28, 2020, 11:07 AM EST Project Member

Labels: Target-79 M-79

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 13 by sheriffbot@chromium.org on Tue, Jan 28, 2020, 11:47 AM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity High. If this is incorrect, please reset the priority. Sheriffbot won't make this change again.

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

Comment 14 by oksamyt@chromium.org on Tue, Jan 28, 2020, 5:27 PM EST Project Member

Looks like SpeechSynthesisUtterance::receiver_ needs to be reset when SpeechSynthesisUtterance is garbage collected. The recommendation is to use a prefinalizer:
https://chromium.googlesource.com/chromium/src/+/HEAD/docs/mojo_ipc_conversion.md#Blink_Specific-Advice
This CL in adjacent code is an example:
https://crrev.com/c/1952085

Comment 15 by sheriffbot@chromium.org on Mon, Feb 3, 2020, 10:41 AM EST Project Member

dmazzoni: 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, Feb 5, 2020, 10:46 AM EST Project Member

Labels: -M-79 M-80 Target-80

Comment 17 by dmazz...@chromium.org on Thu, Feb 6, 2020, 2:24 PM EST Project Member

Status: Started (was: Assigned)

Comment 18 by dmazz...@chromium.org on Thu, Feb 6, 2020, 2:48 PM EST Project Member

I wasn't able to reproduce using the steps in #c9 with an ASAN build on Linux, but the fix seems straightforward:

https://chromium-review.googlesource.com/c/chromium/src/+/2042276

Comment 19 by bugdroid on Thu, Feb 6, 2020, 5:39 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb

commit b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb
Author: Dominic Mazzoni <dmazzoni@chromium.org>
Date: Thu Feb 06 22:38:35 2020

Add pre-finalizer to SpeechSynthesisUtterance.

Avoids a UAF by disconnecting the mojo::Receiver from the pre-finalizer.

~~Bug: 1043603~~
Change-Id: I1592a517bf74dd4fcb8e947e1122442864e0dacc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2042276
Reviewed-by: Darin Fisher <darin@chromium.org>
Commit-Queue: Dominic Mazzoni <dmazzoni@chromium.org>
Cr-Commit-Position: refs/heads/master@{#739140}

[modify] https://crrev.com/b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.cc
[modify] https://crrev.com/b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.h

Comment 20 by dmazz...@chromium.org on Thu, Feb 6, 2020, 7:44 PM EST Project Member

Status: Fixed (was: Started)

Comment 21 by natashapabrai@google.com on Mon, Feb 10, 2020, 2:36 PM EST Project Member

Labels: reward-topanel

Comment 22 by mmoroz@google.com on Tue, Feb 11, 2020, 11:50 AM EST Project Member

Labels: VulnerabilityAnalysis-Requested

dmazzoni@, 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 23 by natashapabrai@google.com on Tue, Feb 11, 2020, 5:08 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 24 by natashapabrai@google.com on Tue, Feb 11, 2020, 5:09 PM EST   Project Member

Congrats! The Panel decided to award $5,000 for this report!

Comment 25 by natashapabrai@google.com on Tue, Feb 11, 2020, 5:18 PM EST   Project Member

Labels: -reward-unpaid reward-inprocess

Comment 26 by adetaylor@google.com on Thu, Feb 13, 2020, 2:31 PM EST   Project Member

Labels: Merge-Request-80 Merge-Request-81

As a high severity security fix, we'd normally merge this to stable. Adding merge labels appropriately. dmazzoni@ - do you feel it's wise to merge this to our next stable refresh, or do you have any stability concerns?

Comment 27 by dmazz...@chromium.org on Fri, Feb 14, 2020, 1:53 PM EST   Project Member

I think we should merge. Thanks.

Comment 28 by adetaylor@google.com on Fri, Feb 14, 2020, 1:54 PM EST   Project Member

Labels: -Merge-Request-80 -Merge-Request-81 Merge-Approved-80 Merge-Approved-81

Great (and I agree the fix looks very straightforward indeed). Please merge to M80 (branch 3987) and M81 (branch 4044).

Comment 29 by dmazz...@chromium.org on Fri, Feb 14, 2020, 2:01 PM EST   Project Member

In the CQ:
https://chromium-review.googlesource.com/c/chromium/src/+/2057526
https://chromium-review.googlesource.com/c/chromium/src/+/2057096

Comment 30 by bugdroid on Fri, Feb 14, 2020, 3:19 PM EST   Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/977e69e5e52718e0a23dd971239313d22be30581

commit 977e69e5e52718e0a23dd971239313d22be30581
Author: Dominic Mazzoni <dmazzoni@chromium.org>
Date: Fri Feb 14 20:17:51 2020

Merge to M80: Add pre-finalizer to SpeechSynthesisUtterance.

Avoids a UAF by disconnecting the mojo::Receiver from the pre-finalizer.

(cherry picked from commit b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb)

~~Bug: 1043603~~
Tbr: darin@chromium.org
Change-Id: I1592a517bf74dd4fcb8e947e1122442864e0dacc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2042276
Reviewed-by: Darin Fisher <darin@chromium.org>
Commit-Queue: Dominic Mazzoni <dmazzoni@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#739140}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2057526
Reviewed-by: Dominic Mazzoni <dmazzoni@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#892}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/977e69e5e52718e0a23dd971239313d22be30581/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.cc
[modify] https://crrev.com/977e69e5e52718e0a23dd971239313d22be30581/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.h

Comment 31 by bugdroid on Fri, Feb 14, 2020, 4:15 PM EST   Project Member

Labels: -merge-approved-81 merge-merged-81 merge-merged-4044

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/3a8ca085146e1be1365931ae2dba98d7f3cd0978

commit 3a8ca085146e1be1365931ae2dba98d7f3cd0978
Author: Dominic Mazzoni <dmazzoni@chromium.org>
Date: Fri Feb 14 21:14:04 2020

Merge to M81: Add pre-finalizer to SpeechSynthesisUtterance.

Avoids a UAF by disconnecting the mojo::Receiver from the pre-finalizer.

(cherry picked from commit b739e83fb99ab2d00d5ed7d029d53d56d42a0fbb)

~~Bug: 1043603~~
Tbr: darin@chromium.org
Change-Id: I1592a517bf74dd4fcb8e947e1122442864e0dacc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2042276
Reviewed-by: Darin Fisher <darin@chromium.org>
Commit-Queue: Dominic Mazzoni <dmazzoni@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#739140}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2057096
Reviewed-by: Dominic Mazzoni <dmazzoni@chromium.org>
Cr-Commit-Position: refs/branch-heads/4044@{#279}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/3a8ca085146e1be1365931ae2dba98d7f3cd0978/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.cc
[modify] https://crrev.com/3a8ca085146e1be1365931ae2dba98d7f3cd0978/third_party/blink/renderer/modules/speech/speech_synthesis_utterance.h

Comment 32 by sheriffbot on Fri, Feb 14, 2020, 7:50 PM EST   Project Member

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

Comment 33 by adetaylor@google.com on Thu, Feb 20, 2020, 12:50 PM EST   Project Member

Labels: Release-2-M80

Comment 34 by adetaylor@google.com on Thu, Feb 20, 2020, 1:00 PM EST   Project Member

Labels: OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

I'm assuming this is cross-platform, for the purposes of release notes.

Comment 35 by adetaylor@chromium.org on Thu, Feb 20, 2020, 1:22 PM EST Project Member

Labels: CVE-2020-6386 CVE_description-missing

Comment 36 by adetaylor@chromium.org on Thu, Feb 27, 2020, 5:53 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 37 by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST Project Member

Cc: achuith@chromium.org

Comment 38 by sheriffbot on Fri, May 15, 2020, 2:56 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