☆ Starred by 5 users

Owner:	rtoy@chromium.org **Email to this user bounced**
CC:	adetaylor@chromium.org prashanthpola@chromium.org rtoy@chromium.org pbomm...@chromium.org hongchan@chromium.org achuith@chromium.org
Status:	Verified *(Closed)*
Components:	Blink>WebAudio
Modified:	Jun 20, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Stability-Memory-AddressSanitizer
Security_Impact-Stable
M-80
Security_Severity-High
allpublic
Unreproducible
ClusterFuzz-Verified
CVE_description-submitted
Target-80
merge-merged-3987
merge-merged-80
merge-merged-4044
merge-merged-81
merge-merged-3987_137
Release-5-M80
CVE-2020-6449

Issue 1059686: UaF in DeferredTaskHandler::BreakConnections(2)

Reported by m...@semmle.com on Mon, Mar 9, 2020, 5:19 AM EDT

Code

VULNERABILITY DETAILS
This issue has the same crash site as 1057593, but the root cause and the fix is different.

Similar to 1057593, when a suspend of the BaseAudioContext and a stop of an AudioScheduleSourceNode happens in the same quantum, the AudioScheduleSourceNode can be destroyed while the BaseAudioContext is suspended. At this point, |active_source_handlers_| in DeferredTaskHandler[1] is responsible for keeping the corresponding AudioScheduleSourceHandler alive before it is used in DeferredTaskHandler::BreakConnections[2].

The code in DeferredTaskHandler::BreakConnections implicitly assumed that |finished_source_handlers_| is a subset of |active_source_handlers_| and hence |active_source_handlers_| is keeping the raw pointers in |finished_source_handlers_| alive. (as can be seen from the |active_source_handlers_.erase|, which assumes |finished| is contained in |active_source_handlers_|)

This problem, however, is that |active_source_handlers_| can be cleared by the DeferredTaskHandler::ClearHandlersToBeDeleted method[3] while |finished_source_handlers_| does not get cleared at the same time, leaving dangling pointers in |finished_source_handlers_|, which will then cause UaF in BreakConnections.

```
  for (auto* finished : finished_source_handlers_) {
    // Break connection first and then remove from the list because that can
    // cause the handler to be deleted.
    finished->BreakConnectionWithLock();     //<-- |active_source_handlers_| may have been cleared, and |finished| is already freed
    active_source_handlers_.erase(finished); //<-- assumes |active_source_handlers_| contains |finished|
  }
```

By destroying the context to trigger BaseAudioContext::Uninitialize, which will then call ClearHandlersToBeDeleted, it is possible to clear |active_source_handlers_| and then trigger |DeferredTaskHandler::BreakConnections| to cause a UaF.

1.
https://source.chromium.org/chromium/chromium/src/+/bf433ad6dcfcaac460512bb45a53d5a2ea5356f9:third_party/blink/renderer/modules/webaudio/deferred_task_handler.h;drc=67e598a2ae32101acac19318c0c56830c12a303f;bpv=1;bpt=1;l=255?originalUrl=https:%2F%2Fcs.chromium.org%2F

2.
https://source.chromium.org/chromium/chromium/src/+/bf433ad6dcfcaac460512bb45a53d5a2ea5356f9:third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc;l=83;drc=67e598a2ae32101acac19318c0c56830c12a303f;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F

3.
https://source.chromium.org/chromium/chromium/src/+/bf433ad6dcfcaac460512bb45a53d5a2ea5356f9:third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc;l=361;drc=67e598a2ae32101acac19318c0c56830c12a303f;bpv=1;bpt=1?originalUrl=https:%2F%2Fcs.chromium.org%2F

VERSION
Chrome version: master branch build 79956ba, asan build 80.3987.132
Operating System: Ubuntu 18.04

REPRODUCTION CASE
Include the attached files finished1.html, finished2.html and test-processor.js in the same directory and then serve it on localhost. Then open finished1.html with a Chromium asan build

```
./out/asan/chrome --js-flags=-expose-gc --user-data-dir=/tmp
```

I've tested this on asan builds of commit 79956ba on the master branch and 80.3987.132. If successful, this should produce asan log like the one attached. Notice that the freed location is different from that of 1057593.

CREDIT INFORMATION
Reporter credit: Man Yue Mo of Github Security Lab

finished1.html
465 bytes View Download

finished2.html
1.1 KB View Download

test-processor.js
356 bytes View Download

asan
21.2 KB View Download

Comment 1 by adetaylor@google.com on Tue, Mar 10, 2020, 11:57 AM EDT Project Member

Cc: rtoy@chromium.org

Comment 2 by rtoy@chromium.org on Tue, Mar 10, 2020, 12:11 PM EDT Project Member

Components: Blink>WebAudio

Comment 3 by rtoy@chromium.org on Tue, Mar 10, 2020, 12:45 PM EDT Project Member

Cc: hongchan@chromium.org

Comment 4 by rtoy@chromium.org on Tue, Mar 10, 2020, 3:00 PM EDT Project Member

Status: Available (was: Unconfirmed)

A linux asan build with the repro test reproduces the crash. Not quite sure yet on how to fix this.

(For some reason, a mac asan build crashes, but doesn't give any stack trace. Don't know why.)

Comment 5 by m...@semmle.com on Tue, Mar 10, 2020, 3:48 PM EDT

Thanks for looking into this and verifying the issue.
As the issue is due to |finished_source_handlers_| and |active_source_handlers_| went out of sync (i.e. |active_source_handlers_| is cleared while |finished_source_handlers_| is not), it seems like the fix should either be
1. clear |finished_source_handlers_| in ClearHandlersToBeDeleted as well when |active_source_handlers_| is cleared; or
2. check that |finished| is contained in |active_source_handlers_| before using it in BreakConnections (although beware that one is raw pointer and one is scoped_refptr)

Either of the above should fix the issue.

Comment 6 by rtoy@chromium.org on Tue, Mar 10, 2020, 3:55 PM EDT Project Member

Yes, I'm looking into option 1 right now. But I may also make finished_source_handlers_ hold scoped_refptrs too instead of raw pointers.

Comment 7 by rtoy@chromium.org on Tue, Mar 10, 2020, 4:05 PM EDT Project Member

It seems making finished_source_handlers_ hold scoped_refptrs is enough. But we should delete them all in ClearHandlersToBeDeleted since everything is going away and we don't want to leave these dangling.

Comment 8 by mpdenton@google.com on Tue, Mar 10, 2020, 9:32 PM EDT Project Member

Labels: Security_Impact-Stable Security_Severity-High OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows

Nice find mmo@. Did you find this with a Semmle query? Would you like to share?

Comment 9 by m...@semmle.com on Wed, Mar 11, 2020, 7:35 AM EDT

Thanks mpdenton@. This one is found by manual inspection. The variants of 1055788 (which in turn is a variant of 977107) can be found with a simple query:

```
from FunctionCall fc, FunctionCall wrapRef
where fc.getTarget().hasName("CrossThreadBindOnce") and
    wrapRef.getTarget().hasName("WrapRefCounted") and
    wrapRef = fc.getAnArgument() and
    exists(Expr e | e.getType().stripType().(Class).getABaseClass*().getName() = "AudioHandler" and
                e = wrapRef.getArgument(0))
select fc, fc.getArgument(0)
```

To look for AudioHandlers that got posted cross thread as a scoped_refptr. The remaining results in the current snapshot are safe either because they check IsExecutionContextDestroyed before using |context_| or they are posted to the audio thread, which does not seem to be able to outlive BaseAudioContext.

Comment 10 by m...@semmle.com on Wed, Mar 11, 2020, 7:43 AM EDT

rtoy@ making |finished_source_handlers_| scoped_refptrs will work and is better than both options that I suggested. The semantics of |active_source_handlers_| and |finished_source_handlers_| are different and relying on |active_source_handlers_| to keep |finished_source_handlers_| alive is error prone, so it is better to make |finished_source_handlers_| scope_refptrs and have it managing its own lifetime.

Comment 11 by ClusterFuzz on Wed, Mar 11, 2020, 11:03 AM EDT Project Member

Labels: Stability-Memory-AddressSanitizer

Detailed Report: https://clusterfuzz.com/testcase?key=5780847096561664

Fuzzer:
Job Type: linux_asan_chrome_mp
Platform Id: linux

Crash Type: Heap-use-after-free READ 4
Crash Address: 0x61200008a9e8
Crash State:
  blink::AudioHandler::BreakConnectionWithLock
  blink::DeferredTaskHandler::BreakConnections
  blink::OfflineAudioContext::HandlePostRenderTasks

Sanitizer: address (ASAN)

Recommended Security Severity: High

Crash Revision: https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&revision=748943

Reproducer Testcase: https://clusterfuzz.com/download?testcase_id=5780847096561664

Additional requirements: Requires HTTP

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/5780847096561664 -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/Yh3qCYFveHj6E5jz5 so we can improve.

Comment 12 by ClusterFuzz on Wed, Mar 11, 2020, 11:11 AM EDT Project Member

Labels: Unreproducible

ClusterFuzz testcase 5780847096561664 appears to be flaky, updating reproducibility label.

Comment 13 by rtoy@chromium.org on Wed, Mar 11, 2020, 11:39 AM EDT Project Member

Status: Started (was: Available)
Owner: rtoy@chromium.org

Comment 14 by sheriffbot on Wed, Mar 11, 2020, 12:53 PM EDT Project Member

Labels: Target-80 M-80

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 15 by sheriffbot on Wed, Mar 11, 2020, 1:34 PM EDT Project Member

Labels: 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 16 by bugdroid on Wed, Mar 11, 2020, 4:24 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/4c57222340cfb78edadf08532f4468c676df5395

commit 4c57222340cfb78edadf08532f4468c676df5395
Author: Raymond Toy <rtoy@chromium.org>
Date: Wed Mar 11 20:23:49 2020

Make finished_source_handlers_ hold scoped_refptrs

Previously, finished_source_handlers_ held raw pointers to
AudioHandlers and assumed that active_source_handlers_ also had a
copy. But when the context goes away, active_source_handlers_ would
be cleared, but not finished_source_handlers_, leaving pointers to
deleted objects.

So do two things:
1. Change finished_source_handlers_ to hold scoped_refptrs to manage
   lifetime of the objects
2. Clear finished_source_handler_ in ClearHandlersToBeDeleted()

Either of these fix the repro case, but let's do both. Don't want to
leaving dangling objects.

Manually tested the repro case which no longer reproduces.

~~Bug: 1059686~~
Change-Id: I2f30c996e8589fa5c3890d32500c4bb4f3bc4286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2098260
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/heads/master@{#749302}

[modify] https://crrev.com/4c57222340cfb78edadf08532f4468c676df5395/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/4c57222340cfb78edadf08532f4468c676df5395/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 17 by ClusterFuzz on Wed, Mar 11, 2020, 9:34 PM EDT Project Member

Status: Verified (was: Started)
Labels: ClusterFuzz-Verified

ClusterFuzz testcase 5780847096561664 is verified as fixed in https://clusterfuzz.com/revisions?job=linux_asan_chrome_mp&range=749269:749271

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

Comment 18 by rtoy@chromium.org on Thu, Mar 12, 2020, 10:56 AM EDT Project Member

Letting this bake for a day. Will probably miss the M82 branch.

Comment 19 by rtoy@chromium.org on Thu, Mar 12, 2020, 10:59 AM EDT Project Member

Hmm. Clusterfuzz says it's fixed and I verified myself that the repro case doesn't occur anymore, but the clusterfuzz range doesn't include the CL. And the CLs in the range seem totally unrelated. Leaving as verified.

Comment 20 by adetaylor@google.com on Thu, Mar 12, 2020, 1:57 PM EDT Project Member

Labels: Merge-Request-81

Let's start the process of merging this back into M81. I'm not sure if it will get into the initial release. Let's not merge until it's baked in Canary for a day, but we can at least get all the Sheriffbotty merge-review questionnaire stuff done.

Comment 21 by sheriffbot on Thu, Mar 12, 2020, 2:01 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: We are only 4 days from stable.
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 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: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 22 by sheriffbot on Thu, Mar 12, 2020, 2:08 PM EDT Project Member

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

Comment 23 by rtoy@chromium.org on Thu, Mar 12, 2020, 2:11 PM EDT Project Member

1. Does your merge fit within the Merge Decision Guidelines?
Yes
2. Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2098260
3. Has the change landed and been verified on master/ToT?
Yes
4. Why are these changes required in this milestone after branch?
Security UaF
5. Is this a new feature?
No

Comment 24 by pbommana@google.com on Thu, Mar 12, 2020, 4:47 PM EDT Project Member

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

+adetaylor@(Security TPM)

Comment 25 by adetaylor@chromium.org on Thu, Mar 12, 2020, 6:16 PM EDT Project Member

Labels: -Merge-Review-81 Merge-Approved-81

Please merge to M81 (branch 4044) so long as it's looking good after a day on Canary.

Comment 26 by rtoy@chromium.org on Fri, Mar 13, 2020, 11:35 AM EDT Project Member

Only see crashes from versions before the fixes for BreakConnections. I think we're ready.

Comment 27 by adetaylor@google.com on Fri, Mar 13, 2020, 1:50 PM EDT Project Member

OK go ahead, thanks!

Comment 28 by adetaylor@google.com on Fri, Mar 13, 2020, 1:51 PM EDT Project Member

(For the benefit of release TPMs - as dicsussed, I'm not approving more merges into M81 just at the moment, but I already approved this one.)

Comment 29 by gov...@chromium.org on Fri, Mar 13, 2020, 1:52 PM EDT Project Member

Re #28: Yeah, it is fine. Thank you.

Comment 30 by bugdroid on Fri, Mar 13, 2020, 3:12 PM EDT 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/+/ff0379405cbceac29b9ad7654e46d873d843e93b

commit ff0379405cbceac29b9ad7654e46d873d843e93b
Author: Raymond Toy <rtoy@chromium.org>
Date: Fri Mar 13 19:10:38 2020

Make finished_source_handlers_ hold scoped_refptrs

Previously, finished_source_handlers_ held raw pointers to
AudioHandlers and assumed that active_source_handlers_ also had a
copy. But when the context goes away, active_source_handlers_ would
be cleared, but not finished_source_handlers_, leaving pointers to
deleted objects.

So do two things:
1. Change finished_source_handlers_ to hold scoped_refptrs to manage
lifetime of the objects
2. Clear finished_source_handler_ in ClearHandlersToBeDeleted()

Either of these fix the repro case, but let's do both. Don't want to
leaving dangling objects.

Manually tested the repro case which no longer reproduces.

(cherry picked from commit 4c57222340cfb78edadf08532f4468c676df5395)

~~Bug: 1059686~~
Change-Id: I2f30c996e8589fa5c3890d32500c4bb4f3bc4286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2098260
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#749302}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2102773
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/4044@{#772}
Cr-Branched-From: a6d9daf149a473ceea37f629c41d4527bf2055bd-refs/heads/master@{#737173}

[modify] https://crrev.com/ff0379405cbceac29b9ad7654e46d873d843e93b/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/ff0379405cbceac29b9ad7654e46d873d843e93b/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 31 by rtoy@chromium.org on Fri, Mar 13, 2020, 5:50 PM EDT Project Member

It appears that the original CL made it into M82, so I think we're done here. No point, I think, in merging to M80.

Comment 32 by adetaylor@chromium.org on Fri, Mar 13, 2020, 6:23 PM EDT Project Member

Agreed. Chances of another M80 release are slim. Thanks.

Comment 33 by adetaylor@google.com on Mon, Mar 16, 2020, 2:13 PM EDT Project Member

Labels: Merge-Approved-80

rtoy@ per your comment on https://bugs.chromium.org/p/chromium/issues/detail?id=1057593#c29, please merge this ASAP to minibranch 3987_137. Please get in touch with govind@ if there is any problem.

Comment 34 by bugdroid on Mon, Mar 16, 2020, 2:28 PM EDT Project Member

Labels: merge-merged-3987_137

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/d044984fa4dac2fa4ac83b3447312a0cff46178e

commit d044984fa4dac2fa4ac83b3447312a0cff46178e
Author: Raymond Toy <rtoy@chromium.org>
Date: Mon Mar 16 18:26:41 2020

Make finished_source_handlers_ hold scoped_refptrs

Previously, finished_source_handlers_ held raw pointers to
AudioHandlers and assumed that active_source_handlers_ also had a
copy. But when the context goes away, active_source_handlers_ would
be cleared, but not finished_source_handlers_, leaving pointers to
deleted objects.

So do two things:
1. Change finished_source_handlers_ to hold scoped_refptrs to manage
   lifetime of the objects
2. Clear finished_source_handler_ in ClearHandlersToBeDeleted()

Either of these fix the repro case, but let's do both. Don't want to
leaving dangling objects.

Manually tested the repro case which no longer reproduces.

(cherry picked from commit 4c57222340cfb78edadf08532f4468c676df5395)

~~Bug: 1050686~~
Change-Id: I2f30c996e8589fa5c3890d32500c4bb4f3bc4286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2098260
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#749302}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2104992
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987_137@{#15}
Cr-Branched-From: 55c16ce255e7a7feca588abeb4f082026b35e1ef-refs/branch-heads/3987@{#989}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/d044984fa4dac2fa4ac83b3447312a0cff46178e/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/d044984fa4dac2fa4ac83b3447312a0cff46178e/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 35 by gov...@chromium.org on Mon, Mar 16, 2020, 8:42 PM EDT Project Member

Approving merge to M80 branch 3987, please merge ASAP. Thank you.

Comment 36 by bugdroid on Tue, Mar 17, 2020, 10:46 AM EDT 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/+/f36c721b7f546ede46bdc57ed9ff1bac3cfb5f9d

commit f36c721b7f546ede46bdc57ed9ff1bac3cfb5f9d
Author: Raymond Toy <rtoy@chromium.org>
Date: Tue Mar 17 14:45:34 2020

Make finished_source_handlers_ hold scoped_refptrs

Previously, finished_source_handlers_ held raw pointers to
AudioHandlers and assumed that active_source_handlers_ also had a
copy. But when the context goes away, active_source_handlers_ would
be cleared, but not finished_source_handlers_, leaving pointers to
deleted objects.

So do two things:
1. Change finished_source_handlers_ to hold scoped_refptrs to manage
   lifetime of the objects
2. Clear finished_source_handler_ in ClearHandlersToBeDeleted()

Either of these fix the repro case, but let's do both. Don't want to
leaving dangling objects.

Manually tested the repro case which no longer reproduces.

(cherry picked from commit 4c57222340cfb78edadf08532f4468c676df5395)

~~Bug: 1050686~~
Change-Id: I2f30c996e8589fa5c3890d32500c4bb4f3bc4286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2098260
Reviewed-by: Hongchan Choi <hongchan@chromium.org>
Commit-Queue: Raymond Toy <rtoy@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#749302}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2107163
Reviewed-by: Raymond Toy <rtoy@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#1016}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/f36c721b7f546ede46bdc57ed9ff1bac3cfb5f9d/third_party/blink/renderer/modules/webaudio/deferred_task_handler.cc
[modify] https://crrev.com/f36c721b7f546ede46bdc57ed9ff1bac3cfb5f9d/third_party/blink/renderer/modules/webaudio/deferred_task_handler.h

Comment 37 by adetaylor@google.com on Tue, Mar 17, 2020, 11:17 AM EDT Project Member

Labels: Release-5-M80

Comment 38 by adetaylor@chromium.org on Tue, Mar 17, 2020, 11:22 AM EDT Project Member

Labels: CVE-2020-6449 CVE_description-missing

Comment 39 by gov...@chromium.org on Tue, Mar 17, 2020, 4:33 PM EDT Project Member

Cc: prashanthpola@chromium.org

Comment 40 by adetaylor@chromium.org on Thu, Mar 19, 2020, 6:30 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 41 by adetaylor@google.com on Wed, Mar 25, 2020, 3:31 PM EDT Project Member

Cc: achuith@chromium.org

Comment 42 by sheriffbot on Sat, Jun 20, 2020, 2:57 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