☆ Starred by 3 users

Owner:	hta@chromium.org
CC:	hbos@chromium.org hta@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebRTC>PeerConnection
Modified:	Jun 18, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

reward-500
Security_Impact-Stable
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-87
Target-87
LTS-Security-86
LTS-Security-NotApplicable-86
external_security_report
merge-merged-4389
merge-merged-89
Release-2-M89
CVE-2021-21191

Issue 1167357: potential uaf in rtc_peer_connection

Reported by wxhu...@gmail.com on Fri, Jan 15, 2021, 5:46 PM 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:
1.Here is my opinion about the rtc_peer_connection, keep in mind that my opinion may be wrong.

https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc;l=3529

- at this function RTCPeerConnection::CloseInternal()

```
void RTCPeerConnection::CloseInternal() {
  '''other code '''
  for (auto& dtls_transport_iter : dtls_transports_by_native_transport_) {
    dtls_transport_iter.value->Close(); // here will use the function  RTCDtlsTransport::Close()
  }

  feature_handle_for_scheduler_.reset();
}
```

And the function
https://source.chromium.org/chromium/chromium/src/+/master:third_party/blink/renderer/modules/peerconnection/rtc_dtls_transport.cc;drc=131697ea2c25234744fe1917571bfa454c2d22cb;l=102

```
void RTCDtlsTransport::Close() {
  closed_from_owner_ = true;
  if (current_state_.state() != webrtc::DtlsTransportState::kClosed) {
    DispatchEvent(*Event::Create(event_type_names::kStatechange)); // wll trige user's javascript code
  }
  ice_transport_->stop();
}
```

the code pattern is similar as https://bugs.chromium.org/p/chromium/issues/detail?id=1107815

What is the expected behavior?

What went wrong?
above all, sorry for no poc now, I will try to make it.

Did this work before? N/A

Chrome version: 87.0.4280.141 Channel: stable
OS Version: 10.0
Flash Version:

Comment 1 by sheriffbot on Fri, Jan 15, 2021, 5:48 PM EST Project Member

Labels: external_security_report

Comment 2 by xinghuilu@chromium.org on Fri, Jan 15, 2021, 7:44 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: hbos@chromium.org
Cc: hta@chromium.org
Labels: Security_Severity-High Security_Impact-Stable
Components: Blink>WebRTC>PeerConnection

Thanks for the report. hbos@, could you take a look on whether this is a potential uaf? Thanks!

Comment 3 by hta@chromium.org on Sat, Jan 16, 2021, 2:23 AM EST Project Member

If I read the other bug correctly, the fear is that one can add a new element to dtls_transports_by_native_transport_ while iterating over the dtls transports.

I don't know why we use an iterator and a list here, though - there should be only one DTLSTransport for each native transport; there's no room in the spec for having more than one. But this may be due to supporting some older code pattern.

Comment 4 by sheriffbot on Sat, Jan 16, 2021, 12:47 PM EST Project Member

Labels: M-87 Target-87

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 5 by sheriffbot on Sat, Jan 16, 2021, 1:27 PM 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 6 by hbos@chromium.org on Mon, Jan 18, 2021, 8:09 AM EST Project Member

Owner: hta@chromium.org
Cc: hbos@chromium.org

dtls_transports_by_native_transport_ uses a WeakMember reference so GC is a risk when JS events fire. I think there was a reason for using WeakMember instead of Member? I have fixed similar bugs by copying the vector and then iterating the copy, in this case the copy would need to use strong Member references to avoid the GC.

Although in this case we could just validate the reference prior to invoking it, right?

Care to own this Harald? I think you introduced this map if I recall correctly

Comment 7 by hta@chromium.org on Mon, Jan 18, 2021, 8:13 AM EST Project Member

I can own this. As I said in #3, I think it's likely that this can't happen, because there can be only one dtls transport, but it seems sensible to use the copy-vector pattern to be 100% safe.

Comment 8 by hta@chromium.org on Wed, Jan 20, 2021, 5:05 AM EST Project Member

Status: Started (was: Assigned)

Comment 9 by bugdroid on Wed, Jan 20, 2021, 5:25 AM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4f62c7bb28b0ce77b773a611c6ba02b361db1c85

commit 4f62c7bb28b0ce77b773a611c6ba02b361db1c85
Author: Harald Alvestrand <hta@chromium.org>
Date: Wed Jan 20 10:23:07 2021

Iterate more carefully over DTLS transports at close

Ensure that even if the set of DTLS transports is modified during
callbacks called from close, the process will be well-defined.

~~Bug: chromium:1167357~~
Change-Id: I712280e7382a647027912178156127831b437f75
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2639893
Reviewed-by: Henrik Boström <hbos@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Commit-Position: refs/heads/master@{#845122}

[modify] https://crrev.com/4f62c7bb28b0ce77b773a611c6ba02b361db1c85/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc

Comment 10 by hta@chromium.org on Wed, Jan 20, 2021, 5:31 AM EST Project Member

Status: Fixed (was: Started)

Asking submitter to consider the change and see if he agrees that it fixes the issue.
Did not come up with an easy way to provoke an UAF here, so no test written.

Comment 11 by wxhu...@gmail.com on Wed, Jan 20, 2021, 6:22 AM EST

Yes, the copy is good

Comment 12 by sheriffbot on Wed, Jan 20, 2021, 12:47 PM EST Project Member

Labels: reward-topanel

Comment 13 by sheriffbot on Wed, Jan 20, 2021, 2:02 PM EST Project Member

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

Comment 14 by amyressler@google.com on Wed, Jan 27, 2021, 6:17 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-500

*** 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 15 by wxhu...@gmail.com on Wed, Jan 27, 2021, 6:49 PM EST

Thanks a lot.But I see that the baseline of high level is 5000.Would you like to tell me the reason?

Comment 16 by amyressler@google.com on Wed, Jan 27, 2021, 7:11 PM EST Project Member

Hi, wxhusst@. Rewards for qualifying security bugs typically range from $500 to $150,000. There is no baseline for a high severity bug report. Decisions made the VRP panel are based on the issue impact, report quality, the proof of concept (if provided), and if there is a functional exploit provided. The Panel decided today on a reward of $500 based on this report. If you would like, I am happy to bring it back to the panel for another discussion next week. In the interim, please tell me how you would like to be credited in release notes.
Additionally a member of our finance team should be reaching out to you shortly to arrange payment. Thank you!

Comment 17 by wxhu...@gmail.com on Wed, Jan 27, 2021, 7:23 PM EST

Thank you.
credit: raven(@raid_akame)
Can I get cve id?

Comment 18 by amyressler@google.com on Wed, Jan 27, 2021, 7:26 PM EST Project Member

Hi, raven! Thank you for your response. CVE number will be updated on this bug when it is assigned. If you track this bug ID, you will be notified of when it is updated with the CVE.

Comment 19 by wxhu...@gmail.com on Wed, Jan 27, 2021, 7:33 PM EST

ok, thank you

Comment 20 by amyressler@google.com on Thu, Jan 28, 2021, 3:10 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 21 by adetaylor@google.com on Wed, Mar 10, 2021, 4:59 PM EST Project Member

Labels: Merge-Approved-89

It's normal for us to merge high severity security bug fixes to stable. Sheriffbot never asked for merge here because of issue 1186797, so adding a merge request to 89 and immediately approving it. Please merge to M89, branch 4389, and we will release this in the next M89 security refresh.

Comment 22 by Git Watcher on Thu, Mar 11, 2021, 1:55 PM EST Project Member

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5651fb858b754b6bdee525b9a0c7b65616c4f93e

commit 5651fb858b754b6bdee525b9a0c7b65616c4f93e
Author: Harald Alvestrand <hta@chromium.org>
Date: Thu Mar 11 18:54:23 2021

[Merge to M89] Iterate more carefully over DTLS transports at close

Ensure that even if the set of DTLS transports is modified during
callbacks called from close, the process will be well-defined.

(cherry picked from commit 4f62c7bb28b0ce77b773a611c6ba02b361db1c85)

~~Bug: chromium:1167357~~
Change-Id: I712280e7382a647027912178156127831b437f75
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2639893
Reviewed-by: Henrik Boström <hbos@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#845122}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2752880
Reviewed-by: Adrian Taylor <adetaylor@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#1521}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/5651fb858b754b6bdee525b9a0c7b65616c4f93e/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection.cc

Comment 23 by adetaylor@google.com on Thu, Mar 11, 2021, 6:17 PM EST Project Member

Labels: Release-2-M89

Comment 24 by adetaylor@google.com on Thu, Mar 11, 2021, 6:19 PM EST Project Member

Labels: CVE-2021-21191 CVE_description-missing

Comment 25 by janag...@google.com on Mon, Mar 15, 2021, 6:58 AM EDT Project Member

Labels: LTS-Security-NotApplicable-86

Comment 26 by amyressler@google.com on Tue, Mar 16, 2021, 10:13 AM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 27 by asumaneev@google.com on Thu, Apr 22, 2021, 10:51 AM EDT Project Member

Labels: LTS-Security-86

Comment 28 by sheriffbot on Fri, Jun 18, 2021, 1:52 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