


☆ Starred by 1 user

Owner:

 [peah@chromium.org](#)
Last visit > 30 days ago

CC:

[hlundin@chromium.org](#)

Status:

Fixed (Closed)

Components:

[Blink>WebRTC>Audio](#)

Modified:

Apr 14, 2020

Backlog-Rank:

Editors:

EstimatedDays:

NextAction:

OS:

[Linux](#), [Android](#), [Windows](#), [Chrome](#), [Mac](#), [Fuchsia](#)

Pri:

2

Type:

[Bug-Security](#)

reward-0

Security_Severity-Low

Security_Impact-Stable

allpublic

a11y-audit

CVE_description-submitted

M-81

Target-81

Release-0-M81

CVE-2020-6444

Issue 922882: Security: Possible load of uninitialized memory in WebRtcAec_Create

Reported by [mlfbr...@stanford.edu](#) on Thu, Jan 17, 2019, 2:08 AM EST

🔗 Code

VULNERABILITY DETAILS

Potential load of uninitialized "aecpc->far_pre_buf" in WebRtcAec_Create

VERSION

Chrome Version: Compiled [aaa99a93e288f0354b03b96588d0624ee910d2ed](#), still exists in source currently.

REPRODUCTION CASE

in WebRtcAec_Create

in src/third_party/webrtc/modules/audio_processing/aec/echo_cancellation.cc, line 122 of your online source code search

(https://cs.chromium.org/chromium/src/third_party/webrtc/modules/audio_processing/aec/echo_cancellation.cc?type=cs&q=WebRtcAec_Create&g=0&i=122)

(NOTE: This depends WebRtcAec_CreateAec failing, which ~means running out of mem)

The gist is that aecpc gets default constructed which does not initialize a field. This field is later potentially loaded

In WebRtcAec_Create:

```
Aec* aecpc = new Aec(); // NOTE: does not initialize aecpc->far_pre_buf
...
aecpc->aec = WebRtcAec_CreateAec(aecpc->instance_count);
if (!aecpc->aec) {
  WebRtcAec_Free(aecpc); // NOTE: the error occurs in this call
```

Follow WebRtcAecFree:

```
Aec* aecpc = reinterpret_cast<Aec*>(aecInst);
...
WebRtc_FreeBuffer(aecpc->far_pre_buf); // NOTE: aecpc->far_pre_buf is uninit
```

Follow WebRtc_FreeBuffer (call with uninit memory):

```
void WebRtc_FreeBuffer(void* handle) {
  RingBuffer* self = (RingBuffer*)handle;
  if (!self) { // NOTE: uninit so self is not false
    return;
  }
  free(self->data); // NOTE: load of uninitialized memory
  free(self);
}
```

CREDIT INFORMATION

Reporter credit: [mlfbrown]

Comment 1 by [mlfbr...@stanford.edu](#) on Thu, Jan 17, 2019, 2:11 AM EST

In short: it appears not exploitable, but would be good to fix

Comment 2 by [jdeblasio@chromium.org](#) on Thu, Jan 17, 2019, 12:36 PM EST Project Member

Status: Assigned (was: Unconfirmed)

Owner: [peah@chromium.org](#)

Cc: [hlundin@chromium.org](#)

Labels: Security_Severity-Low OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows Pri-3

Components: Blink>WebRTC>Audio

This may not even qualify as a security bug, but I'm keeping Restrict-View-SecurityTeam and Bug-Security out of an abundance of caution. That said, I am marking it as low severity and low priority. At least until someone else in Chrome Security who is more opinionated makes a different determination.

[peah@](#), this seems like it might be in your wheelhouse. Can you take ownership of this, or help us find someone else who can? I'm also cc'ing [hlundin@](#) as a backup. Thanks!

Comment 3 by [peah@chromium.org](#) on Thu, Jan 17, 2019, 12:44 PM EST Project Member

Absolutely. I'll look into it. Thanks!

Note that this code is deprecated by the launch of AEC3 but as long as it is still present in the repository it should be addressed.

Comment 4 by [sheriffbot@chromium.org](#) on Fri, Jan 18, 2019, 10:17 AM EST Project Member

Labels: -Pri-3 Pri-2

Comment 5 by [mmoroz@chromium.org](#) on Mon, Apr 29, 2019, 4:40 PM EDT Project Member

Labels: M-76 Security_Impact-Stable

Comment 6 by [sheriffbot@chromium.org](#) on Wed, Sep 11, 2019, 9:03 AM EDT Project Member

Labels: -M-76 M-77 Target-77

Comment 7 by [sheriffbot@chromium.org](#) on Wed, Oct 23, 2019, 9:13 AM EDT Project Member

Labels: -M-77 Target-78 M-78

Comment 8 by [peah@chromium.org](#) on Mon, Dec 9, 2019, 6:22 AM EST Project Member

Since the code in question was removed in the CL <https://webrtc-review.googlesource.com/c/src/+161238>, this issue can now be closed.

Comment 9 by [peah@chromium.org](#) on Mon, Dec 9, 2019, 6:22 AM EST Project Member

Status: Fixed (was: Assigned)

Comment 10 by [sheriffbot@chromium.org](#) on Mon, Dec 9, 2019, 10:46 AM EST Project Member

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

Comment 11 by [awhalley@chromium.org](#) on Wed, Dec 11, 2019, 5:53 PM EST Project Member

Labels: reward-topanel

Comment 12 by [natashapabrai@google.com](#) on Thu, Dec 19, 2019, 12:43 PM EST Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel declined to reward this report

Comment 13 by [adetaylor@google.com](#) on Thu, Jan 30, 2020, 6:31 PM EST Project Member

Labels: -Target-77 -Target-78 -M-78 a11y-audit Target-81 M-81

I'm trying to track down which version this was fixed in such that I can put it in the correct release notes. It was fixed in [a11y-audit](#), which entered webrtc code at position 30050. M80 WebRTC branch was 30022, so I think this didn't make M80 and will instead be in M81.

NB this ticket predates the WebRTC ticket so this is not a duplicate.

Comment 14 by [adetaylor@google.com](#) on Mon, Mar 9, 2020, 6:49 PM EDT Project Member

Labels: Release-0-M81

Comment 15 by [adetaylor@chromium.org](#) on Fri, Mar 13, 2020, 2:32 PM EDT Project Member

Labels: CVE-2020-6444 CVE_description-missing

Comment 16 by [sheriffbot](#) on Mon, Mar 16, 2020, 1:59 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 17 by [adetaylor@chromium.org](#) on Tue, Apr 14, 2020, 3:14 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted