Starred by 3 users

Owner:	hta@chromium.org
CC:	tommi@chromium.org guidou@chromium.org hbos@chromium.org jdeblasio@chromium.org amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebRTC
Modified:	Nov 16, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-08-12
OS:	Linux, Windows, Chrome, Mac, Fuchsia
Pri:	1
Type:	Bug-Security

Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-92
Target-92
external_security_report
merge-merged-4430
merge-merged-90
FoundIn-91
LTS-Merged-90
LTS-Security-90
reward-22000
merge-merged-4515
merge-merged-92
merge-merged-4577
merge-merged-93
LTS-Size-Small
LTS-Complexity-Minimal
reward_to-marcin.towalski_at_gmail.com
Release-2-M92
CVE-2021-30602
merge-merged-4515_132

Issue 1230767: Google Chrome WebRTC addIceCandidate use after free vulnerability (TALOS-2021-1348)

Reported by vulnd...@sourcefire.com on Mon, Jul 19, 2021, 2:37 PM EDT

Code

UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.1.1 Safari/605.1.15

Steps to reproduce the problem:
While executing the attached PoC testcase on Windows 10 x64 machine with ASAN enabled, Chrome crashes inside TrackAddIceCandidate from PeerConnectionTracker.
Snippet of this function is as follows:

```
1:    void PeerConnectionTracker::TrackAddIceCandidate(
2:        RTCPeerConnectionHandler* pc_handler,
3:        RTCIceCandidatePlatform* candidate,
4:        Source source,
5:        bool succeeded) {
6:    DCHECK_CALLED_ON_VALID_THREAD(main_thread_);
7:    int id = GetLocalIDForHandler(pc_handler);
8:    if (id == -1)
9:        return;
10:    String value =
11:        "sdpMid: " + String(candidate->SdpMid()) + ", " + "sdpMLineIndex: " +
12:        (candidate->SdpMLineIndex() ? String::Number(*candidate->SdpMLineIndex())
13:                                    : "null") +
14:        ", " + "candidate: " + String(candidate->Candidate());
```

When setting up an WebRTC session ,function, `AddIceCandidate` is used to add Interactive Connection Establishment candidates, recieved from the remote peer over signaling channle, to browser's ICE agent.

In the supplied PoC , before adding an ICE candidate, garbage collection is forced to mark objects which can later be used because of active Promise that was called before garbage collection.
In between triggering garbage collection and function causing the reuse, allocated memory is accessed thanks to Promise using function `setLocalDescription`.
Function `setLocalDescription` changes the local description associated with the connection which marks parts of the memory to be collected by garbage collector. Same marked memory is accessed during execution of `AddIceCandidate` which constitutes a use after free vulnerability.

With proper manipulation of Promise that is responsible for setting description `setLocalDescription` this vulnerability could lead to control over freed memory and ultimately arbitrary code execution.

Crash Information

Command line :
chrome.exe --js-flags=" --expose-gc" --no-sandbox poc.html
ASAN information Windows 10 x64

```
=================================================================
==26232==ERROR: AddressSanitizer: use-after-poison on address 0x7ef84e666428 at pc 0x7ff654dd0a45 bp 0x0003385fea80 sp 0x0003385feac8
READ of size 8 at 0x7ef84e666428 thread T27
==26232==WARNING: Failed to use and restart external symbolizer!
    #0 0x7ff654dd0a44 in blink::PeerConnectionTracker::TrackAddIceCandidate
```

```
C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\peer_connection_tracker.cc:987
    #1 0x7ff6516d1f5b in base::internal::Invoker<base::internal::BindState<lambda at
../../third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc:1590:7',base::WeakPtr<blink::RTCPeerConnectionHandler>,blink::CrossThreadWeak
Persistent<blink::PeerConnectionTracker>,std::unique_ptr<webrtc::SessionDescriptionInterface,std::default_delete<webrtc::SessionDescriptionInterface>
>,std::unique_ptr<webrtc::SessionDescriptionInterface,std::default_delete<webrtc::SessionDescriptionInterface>
>,std::unique_ptr<webrtc::SessionDescriptionInterface,std::default_delete<webrtc::SessionDescriptionInterface>
>,blink::CrossThreadPersistent<blink::RTCIceCandidatePlatform>,webrtc::RTCError,blink::CrossThreadPersistent<blink::RTCVoidRequest> >,void ()>::RunOnce
C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:690
    #2 0x7ff64f507137 in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:173
    #3 0x7ff651bcadcf in base::sequence_manager::internal::ThreadControllerImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_impl.cc:199
    #4 0x7ff651bcd953 in base::internal::Invoker<base::internal::BindState<void (base::sequence_manager::internal::ThreadControllerImpl::*)
(base::sequence_manager::internal::ThreadControllerImpl::WorkType),base::WeakPtr<base::sequence_manager::internal::ThreadControllerImpl>,base::sequence_manager::
internal::ThreadControllerImpl::WorkType>,void ()>::Run C:\b\s\w\ir\cache\builder\src\base\bind_internal.h:703
    #5 0x7ff64f507137 in base::TaskAnnotator::RunTask C:\b\s\w\ir\cache\builder\src\base\task\common\task_annotator.cc:173
    #6 0x7ff651bcfb24 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:351
    #7 0x7ff651bcf1e9 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:264
    #8 0x7ff64f5a31a0 in base::MessagePumpForUI::DoRunLoop C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:220
    #9 0x7ff64f5a1388 in base::MessagePumpWin::Run C:\b\s\w\ir\cache\builder\src\base\message_loop\message_pump_win.cc:78
    #10 0x7ff651bd10c4 in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::Run
C:\b\s\w\ir\cache\builder\src\base\task\sequence_manager\thread_controller_with_message_pump_impl.cc:460
    #11 0x7ff64f4a3833 in base::RunLoop::Run C:\b\s\w\ir\cache\builder\src\base\run_loop.cc:133
    #12 0x7ff64f54c779 in base::Thread::Run C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:312
    #13 0x7ff64f54cc8e in base::Thread::ThreadMain C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:383
    #14 0x7ff64f5bf66f in base::anonymous namespace'::ThreadFunc C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:111
    #15 0x7ff64f3cd7c7 in asan::AsanThread::ThreadStart C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_thread.cpp:279
    #16 0x7ff93f947033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
    #17 0x7ff9405a2650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

  Address 0x7ef84e666428 is a wild pointer inside of access range of size 0x000000000008.
  SUMMARY: AddressSanitizer: use-after-poison C:\b\s\w\ir\cache\builder\src\third_party\blink\renderer\modules\peerconnection\peer_connection_tracker.cc:987 in
blink::PeerConnectionTracker::TrackAddIceCandidate
  Shadow bytes around the buggy address:
    0x1114c634cc30: 00 00 00 00 00 00 00 00 00 00 f7 f7 f7 f7 f7 f7
    0x1114c634cc40: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 00 00 00 00 00 00
    0x1114c634cc50: 00 00 00 00 00 00 00 00 00 00 f7 f7 f7 f7 f7 f7
    0x1114c634cc60: f7 f7 f7 f7 f7 f7 f7 f7 f7 f7 00 00 00 00 00 00
    0x1114c634cc70: 00 00 00 00 00 00 f7 00 00 00 00 00 00 00 00 00
  =>0x1114c634cc80: 00 00 00 00 f7[f7]f7 f7 f7 f7 f7 f7 f7 f7 f7
    0x1114c634cc90: f7 f7 f7 f7 f7 00 00 00 00 00 00 00 00 00 00 00
    0x1114c634cca0: 00 00 f7 00 00 00 00 00 00 00 00 f7 00 00 00 00
    0x1114c634ccb0: 00 00 00 00 00 00 f7 00 00 00 00 00 00 00 00 00
    0x1114c634ccc0: 00 00 00 00 f7 00 00 00 00 00 00 00 00 00 00 00
    0x1114c634ccd0: 00 00 00 00 f7 00 00 00 00 00 00 00 00 00 f7 00
  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
  Thread T27 created by T0 here:
    #0 0x7ff64f3ce2b2 in asan_wrap_CreateThread C:\b\s\w\ir\cache\builder\src\third_party\llvm\compiler-rt\lib\asan\asan_win.cpp:146
    #1 0x7ff64f5bea6e in base::`anonymous namespace'::CreateThreadInternal C:\b\s\w\ir\cache\builder\src\base\threading\platform_thread_win.cc:171
    #2 0x7ff64f54ba4a in base::Thread::StartWithOptions C:\b\s\w\ir\cache\builder\src\base\threading\thread.cc:187
    #3 0x7ff64e3a0548 in content::RenderProcessHostImpl::Init C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_process_host_impl.cc:1831
    #4 0x7ff64e384308 in content::RenderFrameHostManager::InitRenderView
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:2807
    #5 0x7ff64e37badd in content::RenderFrameHostManager::ReinitializeMainRenderFrame
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:3033
    #6 0x7ff64e37988e in content::RenderFrameHostManager::GetFrameHostForNavigation
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:1057
    #7 0x7ff64e378522 in content::RenderFrameHostManager::DidCreateNavigationRequest
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\render_frame_host_manager.cc:810
    #8 0x7ff64e109166 in content::FrameTreeNode::CreatedNavigationRequest C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\frame_tree_node.cc:538
    #9 0x7ff64e2bcd27 in content::Navigator::Navigate C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigator.cc:578
    #10 0x7ff64e231b74 in content::NavigationControllerImpl::NavigateWithoutEntry
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_controller_impl.cc:3280
    #11 0x7ff64e230d63 in content::NavigationControllerImpl::LoadURLWithParams
C:\b\s\w\ir\cache\builder\src\content\browser\renderer_host\navigation_controller_impl.cc:1116
    #12 0x7ff65532b6dc in content::Shell::LoadURLForFrame C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:251
    #13 0x7ff65532b388 in content::Shell::LoadURL C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:239
    #14 0x7ff65532b08c in content::Shell::CreateNewWindow C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell.cc:229
    #15 0x7ff655372b3a in content::ShellBrowserMainParts::InitializeMessageLoopContext
C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell_browser_main_parts.cc:161
    #16 0x7ff655373114 in content::ShellBrowserMainParts::PreMainMessageLoopRun C:\b\s\w\ir\cache\builder\src\content\shell\browser\shell_browser_main_parts.cc:213
    #17 0x7ff64d91ab56 in content::BrowserMainLoop::PreMainMessageLoopRun C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:959
    #18 0x7ff64e64a9f7 in content::StartupTaskRunner::RunAllTasksNow C:\b\s\w\ir\cache\builder\src\content\browser\startup_task_runner.cc:41
    #19 0x7ff64d91a060 in content::BrowserMainLoop::CreateStartupTasks C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_loop.cc:867
    #20 0x7ff64d921976 in content::BrowserMainRunnerImpl::Initialize C:\b\s\w\ir\cache\builder\src\content\browser\browser_main_runner_impl.cc:131
    #21 0x7ff64d916698 in content::BrowserMain C:\b\s\w\ir\cache\builder\src\content\browser\browser_main.cc:43
    #22 0x7ff64a5a0b8c in content::RunBrowserProcessMain C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:598
    #23 0x7ff64a5a35a9 in content::ContentMainRunnerImpl::RunBrowser C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:1081
    #24 0x7ff64a5a27b1 in content::ContentMainRunnerImpl::Run C:\b\s\w\ir\cache\builder\src\content\app\content_main_runner_impl.cc:956
    #25 0x7ff64a59f9e7 in content::RunContentProcess C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:372
    #26 0x7ff64a59ffe6 in content::ContentMain C:\b\s\w\ir\cache\builder\src\content\app\content_main.cc:398
    #27 0x7ff6476011d2 in main C:\b\s\w\ir\cache\builder\src\content\shell\app\shell_main.cc:33
```

#28 0x7ff65cb54863 in scrt_common_main_seh d:\A01_work\6\s\src\vctools\crt\vcstartup\src\startup\exe_common.inl:288
#29 0x7ff93f947033 in BaseThreadInitThunk+0x13 (C:\Windows\System32\KERNEL32.DLL+0x180017033)
#30 0x7ff9405a2650 in RtlUserThreadStart+0x20 (C:\Windows\SYSTEM32\ntdll.dll+0x180052650)

==26232==ABORTING

What is the expected behavior?

What went wrong?
Summary

A use after free vulnerability exists in the WebRTC functionality of Google Chrome 91.0.4472.114 (Stable) and 93.0.4575.0 (Canary). A specially crafted web page can trigger reuse of previously freed memory which can lead to arbitrary code execution. Victim would need to visit a malicious website to trigger this vulnerability.

Did this work before? N/A

Chrome version: <Copy from: 'about:version'> Channel: n/a
OS Version: OS X 10.14.6

TALOS-2021-1348 - Google_Chrome_WebRTC_addIceCandidate_use_after_free_vulnerability.txt
13.5 KB View Download

poc.html
896 bytes View Download

Comment 1 by sheriffbot on Mon, Jul 19, 2021, 2:40 PM EDT

Labels: external_security_report

Comment 2 by jdeblasio@chromium.org on Mon, Jul 19, 2021, 3:14 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: tommi@chromium.org
Cc: jdeblasio@chromium.org
Labels: -OS-Mac Security_Severity-High FoundIn-91 OS-Windows
Components: Blink>WebRTC

I'm personally unable to repro this right now due to my own Windows env's issue, so I'm just assuming this works.

I think this is a UaF in the renderer [1], so treating it as such. If this is in the browser, this will need to jump up to Security_Severity-Critical.

tommi@: can you please take a look at this? Thanks!

[1] https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/modules/peerconnection/peer_connection_tracker.h;l=40

Comment 3 by sheriffbot on Mon, Jul 19, 2021, 3:16 PM EDT

Labels: Security_Impact-Stable

Comment 4 by sheriffbot on Tue, Jul 20, 2021, 9:06 AM EDT

Labels: M-91 Target-91

Setting milestone and target because of high severity.

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

Comment 5 by sheriffbot on Tue, Jul 20, 2021, 9:06 AM EDT

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 danakj@chromium.org on Fri, Jul 23, 2021, 4:52 PM EDT

Owner: guidou@chromium.org
Cc: tommi@chromium.org

tommi is out for a bit, it seems.

Comment 7 by guidou@chromium.org on Sat, Jul 24, 2021, 3:25 AM EDT

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

Comment 8 by hta@chromium.org on Wed, Jul 28, 2021, 6:31 PM EDT

Unable to reproduce on win-asan bot on ToT - see https://chromium-review.googlesource.com/c/chromium/src/+/3057049

Comment 9 by sheriffbot on Thu, Aug 5, 2021, 1:41 PM EDT

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 10 by sheriffbot on Fri, Aug 6, 2021, 12:21 PM EDT

Labels: -Security_Impact-Extended

Comment 11 by sheriffbot on Fri, Aug 6, 2021, 12:27 PM EDT

Labels: Security_Impact-Extended

Comment 12 by sheriffbot on Fri, Aug 6, 2021, 1:28 PM EDT

Labels: -Security_Impact-Extended Security_Impact-Stable

Comment 13 by vulnd...@sourcefire.com on Fri, Aug 6, 2021, 3:03 PM EDT

Label: reward_to-marcin.towalski_at_gmail.com

Comment 14 by sheriffbot on Sat, Aug 7, 2021, 12:21 PM EDT

Labels: -M-91 Target-92 M-92

Comment 15 by vulnd...@sourcefire.com on Mon, Aug 9, 2021, 12:09 PM EDT

Attaching an updated POC which should make it easier to reproduce. It's a little larger than the original one (that one is minimized) but that's to make it more easily reproducible.

poc-4.html
9.0 KB View Download

Comment 16 by hta@chromium.org on Mon, Aug 9, 2021, 2:02 PM EDT

Asking for more information on the repro:

- Does this repro on any other platform than Windows 10? (We have a scarcity of Windows machines available for testing)
- Does the repro expose the bug every time for you, or is it flaky?

Needed to figure out more on how to proceed.

Comment 17 by vulnd...@sourcefire.com on Mon, Aug 9, 2021, 6:17 PM EDT

- It was mostly tested on Windows but also reproduces on Linux
- It does not reproduce every time, but the latest POC we uploaded should increase success rates

Comment 18 by hta@chromium.org on Tue, Aug 10, 2021, 4:35 AM EDT

Thank you very much!
Able to reproduce on tip-of-tree on Linux with:

- args.gn:

is_asan = true
is_debug = false

- command line

out/asan/chrome --js-flags="--expose-gc" --no-sandbox

Comment 19 by Git Watcher on Tue, Aug 10, 2021, 6:50 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/654536e793760b23679131e9f8db45620e5636c7

commit 654536e793760b23679131e9f8db45620e5636c7
Author: Harald Alvestrand <hta@chromium.org>
Date: Tue Aug 10 10:49:27 2021

Protect candidate better from garbage collection during negotiation.

Includes a test that was reliably observed to produce an UAF on Linux
when compiled with ASAN before the fix.

~~Bug: chromium:1230767~~
Change-Id: I02dd29332a6d00790dcace41b6584b96413ef6f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057049
Reviewed-by: Florent Castelli <orphis@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Commit-Position: refs/heads/master@{#910244}

[modify] https://crrev.com/654536e793760b23679131e9f8db45620e5636c7/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc
[add] https://crrev.com/654536e793760b23679131e9f8db45620e5636c7/third_party/blink/web_tests/fast/peerconnection/poc-123067.html

Comment 20 by hta@chromium.org on Tue, Aug 10, 2021, 7:50 AM EDT

Status: Fixed (was: Assigned)

This CL seems to have fixed the issue. Ran web test and poc-4.html in browser without failure.

Comment 21 by sheriffbot on Tue, Aug 10, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 22 by sheriffbot on Tue, Aug 10, 2021, 1:36 PM EDT

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotifyWebRTC

Comment 23 by sheriffbot on Tue, Aug 10, 2021, 2:01 PM EDT

Labels: Merge-Request-92 Merge-Request-93

Requesting merge to stable M92 because latest trunk commit (910244) appears to be after stable branch point (885287).

Requesting merge to beta M93 because latest trunk commit (910244) appears to be after beta branch point (902210).

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

Comment 24 by amyressler@google.com on Tue, Aug 10, 2021, 3:13 PM EDT

hta@ since this fix just landed earlier today I'm going to decline merge approval to M93 to allow for some bake time for this fix on canary, especially as there will be 93 beta release tomorrow. Please let me know if there are any issues with this. Thanks!

Comment 25 by amyressler@google.com on Tue, Aug 10, 2021, 3:15 PM EDT

Labels: reward_to-marcin.towalski_at_gmail.com

adding reward-to label based on vulndiscovery@ researcher attribution in comment above (in comment # 13)

Comment 26 by hta@chromium.org on Tue, Aug 10, 2021, 5:21 PM EDT

Labels: OS-Chrome OS-Fuchsia OS-Linux OS-Mac
NextAction: 2021-08-12

amyressler@ my reading is that this is going into 94, hasn't made it to a canary release yet, and that we'll ask for a downmerge to 93 in a day or two.
Do you want to decline both merges now and ask me to re-add the merge request labels on Thursday, or should we just leave them dangling?

I don't see it as being extremely urgent, so we'll just roll it when it's ripe.

Comment 27 by hta@chromium.org on Wed, Aug 11, 2021, 1:46 AM EDT

94.0.4604.0 is the first Canary version with the fix.

Comment 28 by sheriffbot on Wed, Aug 11, 2021, 6:53 AM EDT

Labels: -Merge-Request-93 Hotlist-Merge-Review Merge-Review-93

This bug requires manual review: M93'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://chromium.googlesource.com/chromium/src.git/+/main/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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?

5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), govind@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 29 by hta@chromium.org on Wed, Aug 11, 2021, 6:56 AM EDT

1. Yes.
2. https://chromium-review.googlesource.com/c/chromium/src/+/3057049
3. Yes.
4. Yes. Merge to M-92 is desirable.
5. This is a fix for an UAF, which may be a security vulnerability.
6. No.
7. N/A

Comment 30 by amyressler@chromium.org on Thu, Aug 12, 2021, 4:25 PM EDT

hta@ sorry I didn't see your response on Tuesday, but yes, my plan was to leave the merge labels dangling and circle back around. Which is what I'm doing now. :) Approving merge to M93 and since this is a fix for high-severity UAF, going to go ahead and approve this for merge to M92 so this can be included in next week's table channel release. Please merge to M93, branch 4577, and M92, branch 4515, asap. Sorry for getting back around so late today!

Comment 31 by hta@chromium.org on Fri, Aug 13, 2021, 3:07 AM EDT

Labels: -Target-91

I have prepared the merge CLs. Who's supposed to change the label from Merge-Request / Merge-Review to Merge-Approved?

Comment 32 by Git Watcher on Fri, Aug 13, 2021, 6:03 AM EDT

Labels: merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4e02776661c73ce26d04b70ca969063c9e7050e7

commit 4e02776661c73ce26d04b70ca969063c9e7050e7
Author: Harald Alvestrand <hta@chromium.org>
Date: Fri Aug 13 10:02:27 2021

[Merge 92] Protect candidate better from garbage collection during negotiation.

Includes a test that was reliably observed to produce an UAF on Linux
when compiled with ASAN before the fix.

(cherry picked from commit 654536e793760b23679131e9f8db45620e5636c7)

~~Bug: chromium:1230767~~
Change-Id: I02dd29332a6d00790dcace41b6584b96413ef6f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057049
Reviewed-by: Florent Castelli <orphis@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#910244}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3094046
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515@{#2046}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/4e02776661c73ce26d04b70ca969063c9e7050e7/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc
[add] https://crrev.com/4e02776661c73ce26d04b70ca969063c9e7050e7/third_party/blink/web_tests/fast/peerconnection/poc-123067.html

Comment 33 by Git Watcher on Fri, Aug 13, 2021, 6:04 AM EDT

Labels: merge-merged-4577 merge-merged-93

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/19fd0487f0d178112985b5bc1572c5cf71fda890

commit 19fd0487f0d178112985b5bc1572c5cf71fda890
Author: Harald Alvestrand <hta@chromium.org>
Date: Fri Aug 13 10:03:33 2021

[Merge to 93] Protect candidate better from garbage collection during negotiation.

Includes a test that was reliably observed to produce an UAF on Linux
when compiled with ASAN before the fix.

(cherry picked from commit 654536e793760b23679131e9f8db45620e5636c7)

~~Bug: chromium:1230767~~
Change-Id: I02dd29332a6d00790dcace41b6584b96413ef6f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057049
Reviewed-by: Florent Castelli <orphis@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#910244}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3093586
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Cr-Commit-Position: refs/branch-heads/4577@{#779}
Cr-Branched-From: 761ddde228655e313424edec06497d0c56b0f3c4-refs/heads/master@{#902210}

[modify] https://crrev.com/19fd0487f0d178112985b5bc1572c5cf71fda890/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc
[add] https://crrev.com/19fd0487f0d178112985b5bc1572c5cf71fda890/third_party/blink/web_tests/fast/peerconnection/poc-123067.html

Comment 34 by hta@chromium.org on Fri, Aug 13, 2021, 6:23 AM EDT

Cc: amyressler@chromium.org
Labels: -Hotlist-Merge-Review -Merge-Request-92 -Merge-Review-93

Merges done, deleting obsolete labels. Adding sheriff to CC in case I missed something.

Comment 35 by amyressler@google.com on Mon, Aug 16, 2021, 10:11 AM EDT

Labels: Release-2-M92

Comment 36 by amyressler@google.com on Mon, Aug 16, 2021, 10:20 AM EDT

Labels: CVE-2021-30602 CVE_description-missing

Comment 37 by rzanoni@google.com on Thu, Aug 19, 2021, 11:35 AM EDT

Labels: LTS-Security-90 LTS-Merge-Request-90 LTS-Size-Small LTS-Complexity-Minimal

Comment 38 by gianluca@google.com on Fri, Aug 20, 2021, 3:33 AM EDT

Labels: -LTS-Merge-Request-90 LTS-Merge-Approved-90

Comment 39 by hta@chromium.org on Fri, Aug 20, 2021, 4:26 AM EDT

Now we have merges to 93 and 92, and approval for a merge to 90. Is there reason to ask for a merge to 91?

Comment 40 by amyressler@chromium.org on Fri, Aug 20, 2021, 10:45 AM EDT

I don't know about LTS, but for general release channel branches, there is no need to merge to 91. Originally 91 was going to be the first Extended Stable channel release, but that is no longer the case.

Comment 41 by Git Watcher on Fri, Aug 20, 2021, 1:28 PM EDT

Labels: merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/010a318d585ca40546c29263579999aebaf92ee7

commit 010a318d585ca40546c29263579999aebaf92ee7
Author: Harald Alvestrand <hta@chromium.org>
Date: Fri Aug 20 17:27:48 2021

[M90-LTS] Protect candidate better from garbage collection during negotiation.

Includes a test that was reliably observed to produce an UAF on Linux
when compiled with ASAN before the fix.

(cherry picked from commit 654536e793760b23679131e9f8db45620e5636c7)

~~Bug: chromium:1230767~~
Change-Id: I02dd29332a6d00790dcace41b6584b96413ef6f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057049
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#910244}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3102948
Reviewed-by: Artem Sumaneev <asumaneev@google.com>
Owners-Override: Artem Sumaneev <asumaneev@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1570}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/010a318d585ca40546c29263579999aebaf92ee7/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc
[add] https://crrev.com/010a318d585ca40546c29263579999aebaf92ee7/third_party/blink/web_tests/fast/peerconnection/poc-123067.html

Comment 42 by rzanoni@google.com on Mon, Aug 23, 2021, 4:14 AM EDT

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 43 by amyressler@google.com on Wed, Aug 25, 2021, 6:39 PM EDT

Labels: -reward-topanel reward-unpaid reward-22000

*** 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 44 by amyressler@chromium.org on Wed, Aug 25, 2021, 7:06 PM EDT

Congratulations, Marcin! The VRP Panel had decided to award you $22,000 for this report. Thank you for your detailed analysis and reporting +POC of this browser process memory corruption issue in WebRTC. A member of our finance team will be in touch soon to arrange payment. Excellent work and thanks again for this report!

Comment 45 by amyressler@google.com on Thu, Aug 26, 2021, 1:44 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 46 by amyressler@google.com on Fri, Aug 27, 2021, 10:39 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 47 by Git Watcher on Tue, Sep 21, 2021, 5:42 PM EDT

Labels: merge-merged-4515_132

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/43c8a5a2bddd7c1bcb3e0ae1d1bb7ad23ee4395b

commit 43c8a5a2bddd7c1bcb3e0ae1d1bb7ad23ee4395b
Author: Harald Alvestrand <hta@chromium.org>
Date: Tue Sep 21 21:41:04 2021

[Merge 92] Protect candidate better from garbage collection during negotiation.

Includes a test that was reliably observed to produce an UAF on Linux
when compiled with ASAN before the fix.

(cherry picked from commit 654536e793760b23679131e9f8db45620e5636c7)

(cherry picked from commit 4e02776661c73ce26d04b70ca969063c9e7050e7)

~~Bug: chromium:1230767~~
Change-Id: I02dd29332a6d00790dcace41b6584b96413ef6f4
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3057049
Reviewed-by: Florent Castelli <orphis@chromium.org>
Commit-Queue: Harald Alvestrand <hta@chromium.org>
Cr-Original-Original-Commit-Position: refs/heads/master@{#910244}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3094046

Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4515@{#2046}
Cr-Original-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3168970
Auto-Submit: Joe Tessler <jrt@chromium.org>
Reviewed-by: Harald Alvestrand <hta@chromium.org>
Cr-Commit-Position: refs/branch-heads/4515_132@{#8}
Cr-Branched-From: 8e089f9dc0d240f50afd19b527a90447b90ca5bb-refs/branch-heads/4515@{#1934}
Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[add] https://crrev.com/43c8a5a2bddd7c1bcb3e0ae1d1bb7ad23ee4395b/third_party/blink/web_tests/fast/peerconnection/poc-123067.html
[modify] https://crrev.com/43c8a5a2bddd7c1bcb3e0ae1d1bb7ad23ee4395b/third_party/blink/renderer/modules/peerconnection/rtc_peer_connection_handler.cc

Comment 48 by vulnd...@sourcefire.com on Mon, Oct 4, 2021, 3:55 PM EDT

Is there a release date established for this issue? 90 days approaching this month

Comment 49 by amyressler@chromium.org on Mon, Oct 4, 2021, 4:11 PM EDT

Hi vulndiscovery@, the fix for this issue was released in the second security refresh of M92 released on 14 August: https://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop.html

This issue was updated as Fixed on 10 August which, by my math, means this bug will be made public (updated with the allpublic label) by us on or about 16 November 2021.

Comment 50 by vulnd...@sourcefire.com on Mon, Oct 4, 2021, 4:21 PM EDT

Thanks for the update

Comment 51 Deleted

Comment 52 by vulnd...@sourcefire.com on Tue, Nov 16, 2021, 10:37 AM EST

Just following up to see if the all public status will be updated for this issue

Comment 53 by sheriffbot on Tue, Nov 16, 2021, 1:32 PM EST

Labels: -Restrict-View-SecurityNotifyWebRTC 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