Talos Vulnerability Report

TALOS-2021-1348

# Google Chrome WebRTC addIceCandidate use after free vulnerability

NOVEMBER 16, 2021

### CVE NUMBER

CVE-2021-30602

### 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.

### Tested Versions

Google Chrome 91.0.4472.114 (Stable)
Google Chrome 93.0.4575.0 (Canary)

### Product URLs

https://www.google.com/chrome/

### CVSSv3 Score

8.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L

### CWE

CWE-416 - Use After Free

### Details

Google Chrome is a cross-platform web browser, developed by Google.

This vulnerability is in WebRTC, which is a technology that enables websites to capture/stream audio/video and other data between browsers.

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 a WebRTC session, function `AddIceCandidate` is used to add Interactive Connection Establishment candidates, recieved from the remote peer over signaling channel, to the 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 the active Promise that was called before garbage collection. In between triggering garbage collection and the 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. The same marked memory is accessed during execution of `AddIceCandidate` which constitutes a use after free vulnerability.

With proper manipulation of Promise, which 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::CrossThreadWeakPersistent<blink::PeerConnectionTracker>,std::unique_ptr<webrtc::SessionDescriptionInterface,std::default_delete<web
rtc::SessionDescriptionInterface>
>,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>,bas
e::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 f7 00 00 00 00 00 00 00 00
=>0x1114c634cc80: 00 00 00 00 f7[f7]f7 f7 f7 f7 f7 f7 f7 f7 f7 f7
  0x1114c634cc90: f7 f7 f7 f7 f7 f7 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
```

## Timeline

2021-08-06 - Vendor Disclosure

2021-11-16 - Public Release

## CREDIT

Discovered by Marcin Towalski of Cisco Talos.

---

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2021-1334

NEXT REPORT TALOS-2021-1351