Starred by 1 user

Owner: guidou@chromium.org

CC: agpalak@chromium.org
a...@chromium.org
guidou@chromium.org
adetaylor@chromium.org
eladalon@chromium.org
tommi@chromium.org
mfoltz@chromium.org
sergeyu@chromium.org
jophba@chromium.org
w...@chromium.org
ellyj...@chromium.org

Status: Fixed *(Closed)*

Components: UI>Browser>MediaCapture

Modified: Mar 22, 2021

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Windows, Chrome, Mac

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-15000
CVE_description-submitted
M-86
Target-85
Target-86
merge-merged-4240
merge-merged-86
merge-merged-4280
merge-merged-87
Release-2-M86
CVE-2020-16001

Issue 1135018: Security: UaF in TabSharingUI

Reported by chrom...@gmail.com on Sun, Oct 4, 2020, 9:35 PM EDT

Code

Chrome Version: 88.0.4283.0
Operating System: Ubuntu

REPRODUCTION CASE

This is similar to ~~issue 1074796~~.

1. python ./copy_mojo_js_bindings.py /path/to/chrome/.../out/asan/gen
2. python3.6m -m http.server 8605
3. Run chrome with --enable-blink-features=MojoJS
4. Open http://127.0.0.1:8000/poc.html and a new tab, on the first tab (poc.html) select "Chrome tab" in the pop-up dialog box, then try to share the new tab
5. Close the shared tab and wait => crash!

```
=================================================================
==8842==ERROR: AddressSanitizer: heap-use-after-free on address 0x61d000313a98 at pc 0x555563d8f865 bp 0x7fffffffccb0 sp 0x7fffffffcca8
READ of size 8 at 0x61d000313a98 thread T0 (chrome)
[Detaching after fork from child process 11310]
    #0 0x555563d8f864 in begin buildtools/third_party/libc++/trunk/include/vector:1524:30
    #1 0x555563d8f864 in HasObserver base/observer_list.h:303:36
    #2 0x555563d8f864 in AddObserver base/observer_list.h:271:9
    #3 0x555563d8f864 in AddObserver content/browser/web_contents/web_contents_impl.cc:784:14
    #4 0x555563d8f864 in content::WebContentsImpl::AddObserver(content::WebContentsObserver*) content/browser/web_contents/web_contents_impl.cc:2878:14
    #5 0x55556a0f7329 in WebContentsDeviceUsage chrome/browser/media/webrtc/media_stream_capture_indicator.cc:135:9
    #6 0x55556a0f7329 in make_unique<MediaStreamCaptureIndicator::WebContentsDeviceUsage, MediaStreamCaptureIndicator *, content::WebContents *&>
buildtools/third_party/libc++/trunk/include/memory:3043:32
    #7 0x55556a0f7329 in MediaStreamCaptureIndicator::RegisterMediaStream(content::WebContents*, std::__1::vector<blink::MediaStreamDevice,
std::__1::allocator<blink::MediaStreamDevice> > const&, std::__1::unique_ptr<MediaStreamUI, std::__1::default_delete<MediaStreamUI> >)
chrome/browser/media/webrtc/media_stream_capture_indicator.cc:337:13
    #8 0x555573834da9 in TabSharingUIViews::CreateTabCaptureIndicator() chrome/browser/ui/views/tab_sharing/tab_sharing_ui_views.cc:306:37
    #9 0x555573834622 in TabSharingUIViews::OnStarted(base::OnceCallback<void ()>, base::RepeatingCallback<void (content::DesktopMediaID const&)>)
chrome/browser/ui/views/tab_sharing/tab_sharing_ui_views.cc:148:3
    #10 0x55556a0fc148 in MediaStreamCaptureIndicator::UIDelegate::OnStarted(base::OnceCallback<void ()>, base::RepeatingCallback<void (content::DesktopMediaID
const&)>) chrome/browser/media/webrtc/media_stream_capture_indicator.cc:214:19
    #11 0x5555636ae83d in content::MediaStreamUIProxy::Core::OnStarted(long*, bool) content/browser/renderer_host/media/media_stream_ui_proxy.cc:144:23
    #12 0x55556960d563 in Run base/callback.h:100:12
    #13 0x55556960d563 in base::(anonymous namespace)::PostTaskAndReplyRelay::RunTaskAndPostReply(base::(anonymous namespace)::PostTaskAndReplyRelay)
base/threading/post_task_and_reply_impl.cc:97:28
    #14 0x55556960dd54 in Invoke<void (*)(base::(anonymous namespace)::PostTaskAndReplyRelay), base::(anonymous namespace)::PostTaskAndReplyRelay>
base/bind_internal.h:393:12
    #15 0x55556960dd54 in MakeItSo<void (*)(base::(anonymous namespace)::PostTaskAndReplyRelay), base::(anonymous namespace)::PostTaskAndReplyRelay>
base/bind_internal.h:637:12
    #16 0x55556960dd54 in RunImpl<void (*)(base::(anonymous namespace)::PostTaskAndReplyRelay), std::__1::tuple<base::(anonymous
namespace)::PostTaskAndReplyRelay>, 0> base/bind_internal.h:710:12
```

```
    #17 0x55556960dd54 in base::internal::Invoker<base::internal::BindState<void (*)(base::(anonymous namespace)::PostTaskAndReplyRelay), base::(anonymous
namespace)::PostTaskAndReplyRelay>, void ()>::RunOnce(base::internal::BindStateBase*) base/bind_internal.h:679:12
    #18 0x555569589985 in Run base/callback.h:100:12
    #19 0x555569589985 in base::TaskAnnotator::RunTask(char const*, base::PendingTask*) base/task/common/task_annotator.cc:163:33
    #20 0x5555695c127f in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWorkImpl(base::sequence_manager::LazyNow*)
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:332:23
    #21 0x5555695c0aff in base::sequence_manager::internal::ThreadControllerWithMessagePumpImpl::DoWork()
base/task/sequence_manager/thread_controller_with_message_pump_impl.cc:252:36
    #22 0x5555694bcb09 in HandleDispatch base/message_loop/message_pump_glib.cc:374:46
    #23 0x5555694bcb09 in base::(anonymous namespace)::WorkSourceDispatch(_GSource*, int (*)(void*), void*) base/message_loop/message_pump_glib.cc:124:43
    #24 0x7ffff7e42fbc in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51fbc)

0x61d000313a98 is located 536 bytes inside of 2416-byte region [0x61d000313880,0x61d0003141f0)
freed by thread T0 (chrome) here:
    #0 0x55555f1ae4ed in operator delete(void*) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:160:3
    #1 0x555572eedee1 in operator() buildtools/third_party/libc++/trunk/include/memory:2378:5
    #2 0x555572eedee1 in reset buildtools/third_party/libc++/trunk/include/memory:2633:7
    #3 0x555572eedee1 in TabStripModel::SendDetachWebContentsNotifications(TabStripModel::DetachNotifications*) chrome/browser/ui/tabs/tab_strip_model.cc:544:21
    #4 0x555572f08d48 in TabStripModel::CloseWebContentses(base::span<content::WebContents* const, 18446744073709551615ul>, unsigned int)
chrome/browser/ui/tabs/tab_strip_model.cc:1799:5
    #5 0x555572ef41d0 in TabStripModel::InternalCloseTabs(base::span<content::WebContents* const, 18446744073709551615ul>, unsigned int)
chrome/browser/ui/tabs/tab_strip_model.cc:1713:27
    #6 0x555572ef4951 in TabStripModel::CloseWebContentsAt(int, unsigned int) chrome/browser/ui/tabs/tab_strip_model.cc:741:10
    #7 0x55557388e057 in TabStrip::CloseTabInternal(int, CloseTabSource) chrome/browser/ui/views/tabs/tab_strip.cc:2966:16
    #8 0x55557388d999 in TabStrip::CloseTab(Tab*, CloseTabSource) chrome/browser/ui/views/tabs/tab_strip.cc:1817:3
    #9 0x5555738b7bec in Tab::CloseButtonPressed(ui::Event const&) chrome/browser/ui/views/tabs/tab.cc:1040:16
    #10 0x5555710a7fcd in views::ButtonController::OnMouseReleased(ui::MouseEvent const&) ui/views/controls/button/button_controller.cc
    #11 0x55557106c0a4 in ui::ScopedTargetHandler::OnEvent(ui::Event*) ui/events/scoped_target_handler.cc:32:24
    #12 0x55556c8a61b9 in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #13 0x55556c8a61b9 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #14 0x55556c8a5a81 in DispatchEventToTarget ui/events/event_dispatcher.cc:84:14
    #15 0x55556c8a5a81 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #16 0x5555712331d6 in views::internal::RootView::OnMouseReleased(ui::MouseEvent const&) ui/views/widget/root_view.cc:467:9
    #17 0x5555712537c5 in views::Widget::OnMouseEvent(ui::MouseEvent*) ui/views/widget/widget.cc:1292:20
    #18 0x55556c8a61b9 in DispatchEvent ui/events/event_dispatcher.cc:191:12
    #19 0x55556c8a61b9 in ui::EventDispatcher::ProcessEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:140:5
    #20 0x55556c8a5a81 in DispatchEventToTarget ui/events/event_dispatcher.cc:84:14
    #21 0x55556c8a5a81 in ui::EventDispatcherDelegate::DispatchEvent(ui::EventTarget*, ui::Event*) ui/events/event_dispatcher.cc:56:15
    #22 0x55556e887add in ui::EventProcessor::OnEventFromSource(ui::Event*) ui/events/event_processor.cc:49:17
    #23 0x55556e8a3a4f in ui::EventSource::DeliverEventToSink(ui::Event*) ui/events/event_source.cc:113:16
    #24 0x55556e8a366a in ui::EventSource::SendEventToSinkFromRewriter(ui::Event const*, ui::EventRewriter const*) ui/events/event_source.cc:138:12
    #25 0x5555712d7c07 in aura::WindowTreeHostPlatform::DispatchEvent(ui::Event*) ui/aura/window_tree_host_platform.cc:238:38
    #26 0x5555712d2af7 in views::DesktopWindowTreeHostLinux::DispatchEvent(ui::Event*) ui/views/widget/desktop_aura/desktop_window_tree_host_linux.cc:242:29
    #27 0x55556d4435d5 in ui::X11Window::DispatchUiEvent(ui::Event*, x11::Event*) ui/platform_window/x11/x11_window.cc:661:34
    #28 0x55556d442b34 in ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc:605:3
    #29 0x55556d4437ff in non-virtual thunk to ui::X11Window::DispatchEvent(ui::Event* const&) ui/platform_window/x11/x11_window.cc
    #30 0x55556c557d24 in ui::PlatformEventSource::DispatchEvent(ui::Event*) ui/events/platform/platform_event_source.cc:100:29
    #31 0x55556c9ce16d in ui::X11EventSource::DispatchPlatformEvent(ui::Event* const&, x11::Event*) ui/events/platform/x11/x11_event_source.cc:323:3
    #32 0x55556c9d0400 in ui::X11EventSource::ProcessXEvent(x11::Event*) ui/events/platform/x11/x11_event_source.cc:384:5
    #33 0x55556c9d0ae9 in DispatchXEvent ui/events/platform/x11/x11_event_source.cc:453:3
    #34 0x55556c9d0ae9 in non-virtual thunk to ui::X11EventSource::DispatchXEvent(x11::Event*) ui/events/platform/x11/x11_event_source.cc
    #35 0x55556c4e4ce8 in operator() ui/gfx/x/connection.cc:448:15
    #36 0x55556c4e4ce8 in x11::Connection::Dispatch(x11::Connection::Delegate*) ui/gfx/x/connection.cc:475:7
    #37 0x55556c9dfe8b in ui::(anonymous namespace)::XSourceDispatch(_GSource*, int (*)(void*), void*) ui/events/platform/x11/x11_event_watcher_glib.cc:43:15

previously allocated by thread T0 (chrome) here:
    #0 0x55555f1adc8d in operator new(unsigned long) /b/s/w/ir/cache/builder/src/third_party/llvm/compiler-rt/lib/asan/asan_new_delete.cpp:99:3
    #1 0x555563d56359 in content::WebContentsImpl::CreateWithOpener(content::WebContents::CreateParams const&, content::RenderFrameHostImpl*)
content/browser/web_contents/web_contents_impl.cc:1001:7
    #2 0x555563d560d8 in Create content/browser/web_contents/web_contents_impl.cc:515:10
    #3 0x555563d560d8 in content::WebContents::Create(content::WebContents::CreateParams const&) content/browser/web_contents/web_contents_impl.cc:510:10
    #4 0x555572e19bb4 in CreateTargetContents chrome/browser/ui/browser_navigator.cc:436:7
    #5 0x555572e19bb4 in Navigate(NavigateParams*) chrome/browser/ui/browser_navigator.cc:630:28
    #6 0x555573431eb3 in BrowserRootView::OnPerformDrop(ui::DropTargetEvent const&) chrome/browser/ui/views/frame/browser_root_view.cc:252:3
    #7 0x5555712cc12e in views::DropHelper::OnDrop(ui::OSExchangeData const&, gfx::Point const&, int) ui/views/widget/drop_helper.cc:98:21
    #8 0x5555712ec5f1 in OnPerformDrop ui/views/widget/desktop_aura/desktop_native_widget_aura.cc:1240:24
    #9 0x5555712ec5f1 in non-virtual thunk to views::DesktopNativeWidgetAura::OnPerformDrop(ui::DropTargetEvent const&, std::__1::unique_ptr<ui::OSExchangeData,
std::__1::default_delete<ui::OSExchangeData> >) ui/views/widget/desktop_aura/desktop_native_widget_aura.cc
    #10 0x55557130b1e5 in views::DesktopDragDropClientOzone::OnDragDrop(std::__1::unique_ptr<ui::OSExchangeData, std::__1::default_delete<ui::OSExchangeData> >,
int) ui/views/widget/desktop_aura/desktop_drag_drop_client_ozone.cc:272:26
    #11 0x55556d44641f in PerformDrop ui/platform_window/x11/x11_window.cc:913:17
    #12 0x55556d44641f in non-virtual thunk to ui::X11Window::PerformDrop() ui/platform_window/x11/x11_window.cc
    #13 0x55556d44e449 in OnXdndDrop ui/base/x/x11_drag_drop_client.cc:413:35
    #14 0x55556d44e449 in ui::XDragDropClient::HandleXdndEvent(x11::ClientMessageEvent const&) ui/base/x/x11_drag_drop_client.cc:281:5
    #15 0x55556d4292ae in ui::XWindow::ProcessEvent(x11::Event*) ui/base/x/x11_window.cc
    #16 0x55556d44275c in DispatchXEvent ui/platform_window/x11/x11_window.cc:580:12
    #17 0x55556d44275c in non-virtual thunk to ui::X11Window::DispatchXEvent(x11::Event*) ui/platform_window/x11/x11_window.cc
    #18 0x55556c9cf4a0 in ui::X11EventSource::DispatchXEventToXEventDispatchers(x11::Event*) ui/events/platform/x11/x11_event_source.cc:342:22
    #19 0x55556c9d0417 in ui::X11EventSource::ProcessXEvent(x11::Event*) ui/events/platform/x11/x11_event_source.cc:388:5
    #20 0x55556c9d0ae9 in DispatchXEvent ui/events/platform/x11/x11_event_source.cc:453:3
    #21 0x55556c9d0ae9 in non-virtual thunk to ui::X11EventSource::DispatchXEvent(x11::Event*) ui/events/platform/x11/x11_event_source.cc
    #22 0x55556c4e4ce8 in operator() ui/gfx/x/connection.cc:448:15
    #23 0x55556c4e4ce8 in x11::Connection::Dispatch(x11::Connection::Delegate*) ui/gfx/x/connection.cc:475:7
    #24 0x55556c9dfe8b in ui::(anonymous namespace)::XSourceDispatch(_GSource*, int (*)(void*), void*) ui/events/platform/x11/x11_event_watcher_glib.cc:43:15
    #25 0x7ffff7e42e8d in g_main_context_dispatch (/lib/x86_64-linux-gnu/libglib-2.0.so.0+0x51e8d)

SUMMARY: AddressSanitizer: heap-use-after-free buildtools/third_party/libc++/trunk/include/vector:1524:30 in begin
Shadow bytes around the buggy address:
  0x0c3a8005a700: fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa fa
  0x0c3a8005a710: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a720: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a730: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a740: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
=>0x0c3a8005a750: fd fd fd[fd]fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a760: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a770: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a780: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a790: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
  0x0c3a8005a7a0: fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd
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

copy_mojo_js_bindings.py
514 bytes View Download

mojo_bindings.js
163 KB View Download

poc.html
845 bytes View Download

Comment 1 by chrom...@gmail.com on Sun, Oct 4, 2020, 9:44 PM EDT

screen.mp4
5.4 MB View Download

Comment 2 by dominickn@chromium.org on Sun, Oct 4, 2020, 10:36 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: marinaciocea@chromium.org
Cc: guidou@chromium.org
Labels: Security_Severity-High Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>GetUserMedia>Desktop

+TabSharingUI and GetUserMedia folks, can you please take a look at this? Looks like it's in stable; a compromised renderer that can trigger UaF in the browser process is a High severity security issue.

Comment 3 by guidou@chromium.org on Mon, Oct 5, 2020, 3:06 AM EDT

Owner: agpalak@chromium.org
Components: UI>Browser>TabCapture

agpalak@

Comment 4 by guidou@chromium.org on Mon, Oct 5, 2020, 3:06 AM EDT

agpalak@: Can you take a look?

Comment 5 by sheriffbot on Mon, Oct 5, 2020, 1:58 PM EDT

Labels: Target-85 M-85

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 6 by agpalak@chromium.org on Tue, Oct 6, 2020, 5:26 AM EDT

Cc: eladalon@chromium.org

Comment 7 by sheriffbot on Wed, Oct 7, 2020, 1:36 PM EDT

Labels: -M-85 M-86 Target-86

Comment 8 by chrom...@gmail.com on Mon, Oct 12, 2020, 7:59 AM EDT

Any update on this bug? Thanks!

Comment 9 by agpalak@chromium.org on Tue, Oct 13, 2020, 4:46 AM EDT

Cc: agpalak@chromium.org

Comment 10 by agpalak@chromium.org on Tue, Oct 13, 2020, 4:46 AM EDT

Owner: guidou@chromium.org

Comment 11 Deleted

Comment 12 by guidou@chromium.org on Wed, Oct 14, 2020, 2:51 PM EDT

Cc: a...@chromium.org

Comment 13 by bugdroid on Wed, Oct 14, 2020, 3:44 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/229fdaf8fc05e0eeadad380d401c191afd822d92

commit 229fdaf8fc05e0eeadad380d401c191afd822d92
Author: Guido Urdaneta <guidou@chromium.org>
Date: Wed Oct 14 19:40:12 2020

Validate input of MediaStreamDispatcherHost::OpenDevice()

This method forwards to MediaStreamManager::OpenDevice(), which
DCHECKs for the stream type to be device video or audio capture
(i.e., webcam or mic). However, MSDH admits other stream types,
which cause MSM::OpenDevice to hit this DCHECK.

This CL ensures that a message containing an incorrect stream type,
which could be sent by a malicious renderer, results in killing the
renderer process.

~~Bug: 1135018~~
Change-Id: I3884dde95d92c41f44966a8ab1dd7bdfd4b23b9b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2472397
Auto-Submit: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Guido Urdaneta <guidou@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/master@{#817151}

[modify] https://crrev.com/229fdaf8fc05e0eeadad380d401c191afd822d92/content/browser/bad_message.h
[modify] https://crrev.com/229fdaf8fc05e0eeadad380d401c191afd822d92/content/browser/renderer_host/media/media_stream_dispatcher_host.cc
[modify] https://crrev.com/229fdaf8fc05e0eeadad380d401c191afd822d92/tools/metrics/histograms/enums.xml

Comment 14 by guidou@chromium.org on Wed, Oct 14, 2020, 6:43 PM EDT

Status: Fixed (was: Assigned)

Comment 15 by guidou@chromium.org on Wed, Oct 14, 2020, 6:45 PM EDT

Labels: Merge-Request-87

Comment 16 by sheriffbot on Thu, Oct 15, 2020, 3:08 PM EDT

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

Comment 17 by sheriffbot on Thu, Oct 15, 2020, 3:47 PM EDT

Labels: -Merge-Request-87 Merge-Review-87 Hotlist-Merge-Review

This bug requires manual review: M87'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/+/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 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), bindusuvarna @(iOS), cindyb@(ChromeOS), lakpamarthy@(Desktop)

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

Comment 18 by lakpamarthy@google.com on Fri, Oct 16, 2020, 7:31 PM EDT

guidou@ - can you please address the merge questionnaire to consider this for M87? Thanks!

Comment 19 by adetaylor@google.com on Sun, Oct 18, 2020, 4:52 PM EDT

Labels: reward-topanel

Comment 20 by adetaylor@google.com on Sun, Oct 18, 2020, 4:56 PM EDT

Labels: Merge-Request-86

Comment 21 by guidou@chromium.org on Mon, Oct 19, 2020, 9:22 AM EDT

Cc: adetaylor@chromium.org

Comment 22 by guidou@chromium.org on Mon, Oct 19, 2020, 9:24 AM EDT

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/+/2472397

3. Has the change landed and been verified on ToT?
Yes.

4. Does this change need to be merged into other active release branches (M-1, M+1)?
We should consider merging to M86, if a respin is planned.

5. Why are these changes required in this milestone after branch?
To fix a security issue.

6. Is this a new feature?
No.

7. If it is a new feature, is it behind a flag using finch?
N/A

Comment 23 by adetaylor@chromium.org on Mon, Oct 19, 2020, 10:27 AM EDT

Labels: -Merge-Request-86 -Merge-Review-87 Merge-Approved-87 Merge-Approved-86

Approving merge to M87, branch 4280, and M86, branch 4240, assuming no problems have appeared in Canary.

Comment 24 by bugdroid on Mon, Oct 19, 2020, 1:12 PM EDT

Labels: -merge-approved-87 merge-merged-87 merge-merged-4280

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/2bf28a4ef7c8cc5d544f23039eb9574ae9aedd6b

commit 2bf28a4ef7c8cc5d544f23039eb9574ae9aedd6b
Author: Guido Urdaneta <guidou@chromium.org>
Date: Mon Oct 19 17:11:22 2020

Validate input of MediaStreamDispatcherHost::OpenDevice()

This method forwards to MediaStreamManager::OpenDevice(), which
DCHECKs for the stream type to be device video or audio capture
(i.e., webcam or mic). However, MSDH admits other stream types,
which cause MSM::OpenDevice to hit this DCHECK.

This CL ensures that a message containing an incorrect stream type,
which could be sent by a malicious renderer, results in killing the
renderer process.

(cherry picked from commit 229fdaf8fc05e0eeadad380d401c191afd822d92)

~~Bug: 1135018~~
Change-Id: I3884dde95d92c41f44966a8ab1dd7bdfd4b23b9b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2472397
Auto-Submit: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Guido Urdaneta <guidou@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#817151}
TBR: avi@chromium.org
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2485055
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Cr-Commit-Position: refs/branch-heads/4280@{#493}
Cr-Branched-From: ea420fb963f9658c9969b6513c56b8f47efa1a2a-refs/heads/master@{#812852}

[modify] https://crrev.com/2bf28a4ef7c8cc5d544f23039eb9574ae9aedd6b/content/browser/bad_message.h
[modify] https://crrev.com/2bf28a4ef7c8cc5d544f23039eb9574ae9aedd6b/content/browser/renderer_host/media/media_stream_dispatcher_host.cc
[modify] https://crrev.com/2bf28a4ef7c8cc5d544f23039eb9574ae9aedd6b/tools/metrics/histograms/enums.xml

Comment 25 by bugdroid on Mon, Oct 19, 2020, 1:16 PM EDT

Labels: -merge-approved-86 merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/740285102aa1c160151e0470a496fdc81a7e1cd4

commit 740285102aa1c160151e0470a496fdc81a7e1cd4
Author: Guido Urdaneta <guidou@chromium.org>
Date: Mon Oct 19 17:15:33 2020

Validate input of MediaStreamDispatcherHost::OpenDevice()

This method forwards to MediaStreamManager::OpenDevice(), which
DCHECKs for the stream type to be device video or audio capture
(i.e., webcam or mic). However, MSDH admits other stream types,
which cause MSM::OpenDevice to hit this DCHECK.

This CL ensures that a message containing an incorrect stream type,
which could be sent by a malicious renderer, results in killing the
renderer process.

(cherry picked from commit 229fdaf8fc05e0eeadad380d401c191afd822d92)

~~Bug: 1135018~~
Change-Id: I3884dde95d92c41f44966a8ab1dd7bdfd4b23b9b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2472397
Auto-Submit: Guido Urdaneta <guidou@chromium.org>
Commit-Queue: Guido Urdaneta <guidou@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#817151}
TBR: avi@chromium.org
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2485092
Reviewed-by: Guido Urdaneta <guidou@chromium.org>
Cr-Commit-Position: refs/branch-heads/4240@{#1277}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/740285102aa1c160151e0470a496fdc81a7e1cd4/content/browser/bad_message.h
[modify] https://crrev.com/740285102aa1c160151e0470a496fdc81a7e1cd4/content/browser/renderer_host/media/media_stream_dispatcher_host.cc
[modify] https://crrev.com/740285102aa1c160151e0470a496fdc81a7e1cd4/tools/metrics/histograms/enums.xml

Comment 26 by adetaylor@google.com on Mon, Oct 19, 2020, 11:09 PM EDT

Labels: Release-2-M86

Comment 27 by adetaylor@google.com on Wed, Oct 21, 2020, 7:12 PM EDT

Labels: -reward-topanel reward-unpaid reward-15000

*** 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 28 by adetaylor@google.com on Wed, Oct 21, 2020, 7:19 PM EDT

Congratulations, the VRP panel has decided to award $15,000 for this bug.

Comment 29 by adetaylor@google.com on Thu, Oct 22, 2020, 12:26 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 30 by adetaylor@google.com on Sun, Dec 6, 2020, 12:59 AM EST
Labels: CVE-2020-16001 CVE_description-missing

Comment 31 by adetaylor@google.com on Thu, Jan 7, 2021, 2:03 PM EST
Labels: -CVE_description-missing CVE_description-submitted

Comment 32 by sheriffbot on Thu, Jan 21, 2021, 1:51 PM EST
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 33 by mfoltz@chromium.org on Mon, Mar 22, 2021, 7:55 PM EDT
Components: UI>Browser>MediaCapture

Comment 34 by mfoltz@chromium.org on Mon, Mar 22, 2021, 7:55 PM EDT
Components: -UI>Browser>TabCapture