Starred by 2 users

Owner:	mfoltz@chromium.org **OOO until 1/3**
CC:	glazunov@google.com adetaylor@chromium.org rdevl...@chromium.org geo...@google.com sheriffbot solomonkinard@chromium.org mfoltz@chromium.org tjudkins@chromium.org wfh@chromium.org creis@chromium.org ajgo@chromium.org taku...@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Sandbox>SiteIsolation Internals>Cast Platform>Extensions
Modified:	May 20, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Chrome
Pri:	1
Type:	Bug-Security

reward-0
Security_Impact-Stable
Security_Severity-Medium
M-80
allpublic
Disable-Nags
CVE_description-submitted
Target-80
reward_to-glazunov_at_google.com
Release-0-M83
CVE-2020-6485

Blocking: ~~Issue 1031679~~

Issue 1047285: Security of media-router built-in extension relies on untrustworthy MessageSender.id

Reported by lukasza@chromium.org on Thu, Jan 30, 2020, 1:08 PM EST Project Member

Code

This is a media-router-specific follow-up to ~~issue 1032159~~.

glazunov@ points out that some component extensions try to allowlist certain security-sensitive operations based on *untrustworthy* MessageSender.id. See:
https://cs.chromium.org/chromium/src/chrome/browser/resources/media_router/extension/src/external_message_listener.js?rcl=29324b698ccd8920bc81c71d42dadc6310f0ad0f&l=75

We should switch to using a (trustworthy) MessageSender.origin instead. If the extension message is sent from an extension frame or background page, then both MessageSender.origin and MessageSender.id should be the same (with "chrome-extension://" prepended to MessageSender.origin) - in this case the change should be straightforward (although I had trouble figuring out how to actually make changes - the external_message_listener.js file doesn't seem to be covered by Chromium repo).

If the extension message may be send from a content script, then:
1) MessageSender.origin (the origin of the web frame where the content script was injected into) may differ from MessageSender.id (the id of the extension that the content script belongs to).
2) Web renderers are inherently able to spoof content scripts that may be injected into them - there may not be much we can do here.

Comment 1 by lukasza@chromium.org on Thu, Jan 30, 2020, 1:10 PM EST Project Member

Status: Assigned (was: Untriaged)
Owner: mfoltz@chromium.org

mfoltz@, could you PTAL as one of //chrome/browser/media/router/OWNERS?
(could you also help set the appropriate OS labels/checkboxes for this bug?)

Comment 2 by mfoltz@chromium.org on Thu, Jan 30, 2020, 1:25 PM EST Project Member

I'm not familiar with our usage of MessageSender.id. I'll have to do some sleuthing to figure out who might be familiar with this particular code path.

Comment 3 by mfoltz@chromium.org on Thu, Jan 30, 2020, 2:08 PM EST Project Member

Labels: OS-Chrome

Comment 4 by sheriffbot@chromium.org on Fri, Jan 31, 2020, 11:18 AM EST Project Member

Labels: Target-80 M-80

Setting milestone and target because of Security_Impact=Stable and medium severity.

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

Comment 5 by lukasza@chromium.org on Mon, Feb 3, 2020, 12:50 PM EST Project Member

I note that |sender.id| is also dereferenced in chrome/browser/resources/media_router/extension/src/internal_message_listener.js in the validateEvent function.

Comment 6 by mfoltz@chromium.org on Mon, Feb 3, 2020, 4:46 PM EST Project Member

That's internal messaging between extension frames, not content scripts or sites. I can clean that up but it's not the same security issue as external messaging.

Comment 7 by bugdroid on Mon, Feb 3, 2020, 5:20 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/def6cddc03bfff5182e28b272dad3f2e90e30270

commit def6cddc03bfff5182e28b272dad3f2e90e30270
Author: mark a. foltz <mfoltz@chromium.org>
Date: Mon Feb 03 22:19:55 2020

Roll src/chrome/browser/resources/media_router/extension/src/ 29324b698..7835fcd45 (27 commits)

https://chromium.googlesource.com/media_router.git/+log/29324b698ccd..7835fcd45668

$ git log 29324b698..7835fcd45 --date=short --no-merges --format='%ad %ae %s'
2020-02-03 mfoltz [Cast Extension] Update files.gni.
2020-01-31 mfoltz [Media Router] Convert external_message_listener to use sender.origin.
2020-01-13 mfoltz Remove DIAL MRP
2020-01-07 mfoltz [MR extension] Lower the severity of provideSinks(): provider not found error
2020-01-06 mfoltz Add explicit '!' for non-null types as required by http://go/js-nullability
2019-12-04 mfoltz Delete invalid goog.provide'd namespace initialization
2019-11-27 mfoltz Don't load disabled extension MediaRouteProviders
2019-10-29 mfoltz Fix typo in unit_test_utils.js.
2019-10-09 mfoltz Fix or suppress upcoming JSCompiler type errors
2019-09-09 mfoltz Removed obsolete "cloud on" setting.
2019-09-05 mfoltz Removed log spam related to Weave being unavailable.
2019-09-05 mfoltz Re-ran genjsdeps.
2019-07-25 mfoltz [Media Router] Log finch experiments to feedback PSDs
2019-07-12 mfoltz Modify route creation metrics in extension DIAL MRP
2019-06-28 mfoltz [Mirroring Service] Remove audio checkbox from desktop picker
2019-06-21 mfoltz Make Media Router component extension tests support Jasmine 3
2019-06-18 mfoltz [MR extension] Don't call chooseDesktopMedia() with a tab ID
2019-06-10 mfoltz [Media Router component extension] Log feature states in feedback logs
2019-05-25 mfoltz [Media Router] Revise capture resolution selection algorithm.
2019-05-14 mfoltz Record MediaRouter.Dial.ParseMessage in DialProviderWrapper
2019-05-02 mfoltz Update metrics collection in DIAL MRP
2019-05-02 mfoltz Fix MirrorMediaStream test failure where mediaDevices is not defined
2019-04-18 mfoltz Fix a crash in mr.mirror.Session's constructor
2019-04-17 mfoltz Disable Adaptive Latency for Cast Mirroring. There are audio bugs caused by this feature.
2019-04-15 mfoltz Set route description in the ctor of mr.mirror.Session
2019-02-22 mfoltz Ads classes for the Web Sender
2019-01-08 mfoltz Fixes various potential XSS vulnerabilities in the MR extension.

Created with:
roll-dep src/chrome/browser/resources/media_router/extension/src
R=takumif@chromium.org

~~Bug: 1047285~~
Change-Id: Ic02e060e44323be3b44a86fcc3a84f7e43b60683
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2036436
Reviewed-by: Takumi Fujimoto <takumif@chromium.org>
Commit-Queue: mark a. foltz <mfoltz@chromium.org>
Cr-Commit-Position: refs/heads/master@{#737949}

[modify] https://crrev.com/def6cddc03bfff5182e28b272dad3f2e90e30270/DEPS

Comment 8 by mfoltz@chromium.org on Mon, Feb 3, 2020, 5:21 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 9 by sheriffbot@chromium.org on Tue, Feb 4, 2020, 12:16 PM EST Project Member

Labels: Restrict-View-SecurityNotify

Comment 10 by creis@chromium.org on Tue, Feb 4, 2020, 12:35 PM EST Project Member

Components: Internals>Sandbox>SiteIsolation

Thanks for the quick fix!

Comment 11 by bugdroid on Tue, Feb 4, 2020, 4:36 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/eaac8929395dbfecaf47c45bfb7726be03afc02f

commit eaac8929395dbfecaf47c45bfb7726be03afc02f
Author: mark a. foltz <mfoltz@chromium.org>
Date: Tue Feb 04 21:35:33 2020

Roll src/chrome/browser/resources/media_router/extension/src/ 7835fcd45..d4389c097 (1 commit)

https://chromium.googlesource.com/media_router.git/+log/7835fcd45668..d4389c097c61

$ git log 7835fcd45..d4389c097 --date=short --no-merges --format='%ad %ae %s'
2020-02-04 mfoltz [Cast Extension] Fix mr.InternalMessageListener to use sender.origin.

Created with:
roll-dep src/chrome/browser/resources/media_router/extension/src
R=takumif@chromium.org

~~Bug: 1047285~~
Change-Id: Ieb414c70d4ad25844a4d4634ec24710670d7d9bc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2036884
Reviewed-by: Takumi Fujimoto <takumif@chromium.org>
Commit-Queue: mark a. foltz <mfoltz@chromium.org>
Cr-Commit-Position: refs/heads/master@{#738343}

[modify] https://crrev.com/eaac8929395dbfecaf47c45bfb7726be03afc02f/DEPS

Comment 12 by adetaylor@google.com on Mon, Mar 23, 2020, 4:53 PM EDT Project Member

Labels: reward_to-glazunov_at_google.com

Comment 13 by natashapabrai@google.com on Mon, Mar 30, 2020, 12:59 PM EDT Project Member

Labels: reward-topanel

Comment 14 by sheriffbot on Mon, Mar 30, 2020, 2:21 PM EDT Project Member

Labels: Merge-Request-81

Requesting merge to beta M81 because latest trunk commit (738343) appears to be after beta branch point (737173).

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

Comment 15 by sheriffbot on Mon, Mar 30, 2020, 2:23 PM EDT Project Member

Labels: -Merge-Request-81 Merge-Review-81 Hotlist-Merge-Review

This bug requires manual review: We are only 7 days from stable.
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 master/ToT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

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

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

Comment 16 by geo...@google.com on Mon, Mar 30, 2020, 6:08 PM EDT Project Member

Labels: -Merge-Review-81 Merge-Approved-81

Approved M81

Comment 17 by natashapabrai@google.com on Wed, Apr 1, 2020, 6:20 PM EDT Project Member

Labels: -reward-topanel reward-0

The Panel declined to award this report

Comment 18 by sheriffbot on Fri, Apr 3, 2020, 12:08 PM EDT Project Member

Cc: sheriffbot geo...@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 19 by sheriffbot on Mon, Apr 6, 2020, 12:10 PM EDT Project Member

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 20 by rdevl...@chromium.org on Mon, Apr 6, 2020, 6:18 PM EDT Project Member

Cc: adetaylor@chromium.org

It looks like mfoltz is out for awhile. It doesn't look like this was merged to M81 yet, but since it's a roll, I'm not sure how easy/reasonable that is.

takumif@ (reviewer of the original CL) and adetaylor@, mind figuring the best course of action here?

Comment 21 by taku...@chromium.org on Mon, Apr 6, 2020, 6:36 PM EDT Project Member

Labels: Disable-Nags

The Media Router component extension is built in google3 (google3/chrome_platform/media_router/extension/), and IIRC has a subset of its code rolled into Chromium to allow some automated testing. Since the extension code in the Chromium repo doesn't get shipped, a cherry-pick wouldn't do much. The M81 component extension built from the google3 code already contains the fix, so no further action is needed.

Comment 22 by adetaylor@chromium.org on Tue, Apr 7, 2020, 12:00 AM EDT Project Member

Labels: -Hotlist-Merge-Review -Merge-Approved-81

Re #c21 thank you takumif@. Removing merge tags then. I'll still credit this in release notes at some point, but it's probably too late for M81.

Comment 23 by sheriffbot on Tue, May 12, 2020, 2:53 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 24 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 25 by adetaylor@chromium.org on Mon, May 18, 2020, 11:59 AM EDT Project Member

Labels: CVE-2020-6485 CVE_description-missing

Comment 26 by adetaylor@chromium.org on Wed, May 20, 2020, 11:44 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted