Starred by 1 user

| | |
|---|---|
| **Owner:** | taku...@chromium.org |
| **CC:** | rzanoni@google.com<br>jrw@chromium.org<br>steimel@chromium.org<br>muyaoxu@google.com<br>mfoltz@chromium.org<br>ahmedmoussa@google.com<br>taku...@chromium.org |
| **Status:** | Verified *(Closed)* |
| **Components:** | Internals>Cast>UI |
| **Modified:** | Jul 29, 2022 |
| **Backlog-Rank:** | ---- |
| **Editors:** | ---- |
| **EstimatedDays:** | ---- |
| **NextAction:** | ---- |
| **OS:** | Linux, Windows, Chrome, Mac, Fuchsia |
| **Pri:** | 1 |
| **Type:** | Bug-Security |

Hotlist-Merge-Review
Security_Severity-High
allpublic
CVE_description-submitted
M-98
Target-98
FoundIn-98
Security_Impact-Extended
merge-merged-4664
LTS-Merge-Merged-96
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1131

# Issue 1297404: Security: heap-use-after-free in global_media_controls::MediaItemManagerImpl::HideItem

Reported by abalq...@microsoft.com on Mon, Feb 14, 2022, 9:25 PM EST

Code

**VULNERABILITY DETAILS**
Browser process crashes when hiding a specific type of media control.

**VERSION**
Chrome Version: 100.0.4890.0 (Developer Build) (64-bit)
Operating System: Windows 11 (dual monitor setup)

**REPRODUCTION CASE**
This seems to only trigger with dual monitor setup. So when the media control appears without dual monitors it does not show an extra option in the dialog that selects the screen. Somehow that button is important.

1. Download attached extension files into a folder like in 'C:/ext/' (run manually install)
2. Run:
./chrome.exe --user-data-dir="C:/profiles/poc" --disable-extensions-except="C:/ext/" --load-extension="C:/ext/" --no-first-run --enable-logging=stderr about:blank
3. Wait a few minutes and crash should occur

**FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION**
Type of crash: browser
Crash State: See attached ASAN log `mediasan.txt`

**CREDIT INFORMATION**
Reporter credit: Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research

**mediasan.txt**
16.9 KB View Download

**service_worker.js**
10.1 KB View Download

**manifest.json**
388 bytes View Download

Comment 1 by abalq...@microsoft.com on Mon, Feb 14, 2022, 9:38 PM EST

For step 1 of repro: "run manually install" supposed to be "or manually install"

Comment 2 by adetaylor@google.com on Mon, Feb 14, 2022, 9:45 PM EST Project Member

Thanks for the report! I don't have a multi-monitor Windows setup so we'll take a look into this tomorrow.

Comment 3 by abalq...@microsoft.com on Mon, Feb 14, 2022, 10:55 PM EST

I ran it again without dual monitor for good measure and it reproduced. Sorry its been a long day chasing this bug.

Comment 4 by adetaylor@google.com on Tue, Feb 15, 2022, 2:02 PM EST Project Member

**Labels:** FoundIn-98 Security_Severity-High Pri-1

Nice! Thanks for doing so much work on the repro! I was able to reproduce this on Windows first time using win32-release_x64_asan-win32-release_x64-950353.

As a browser process crash, this would be Critical severity, but mitigated down to High by the need for an extension.

Comment 5 by adetaylor@google.com on Tue, Feb 15, 2022, 2:04 PM EST Project Member

**Owner:** steimel@chromium.org
**Cc:** jrw@chromium.org
**Labels:** OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows
**Components:** Internals>Cast>UI

steimel@, please could you take a look?

(Tagging with all desktop platforms - please adjust as necessary)

Comment 6 by sheriffbot on Tue, Feb 15, 2022, 2:05 PM EST Project Member

**Labels:** Security_Impact-Extended

Comment 7 by sheriffbot on Tue, Feb 15, 2022, 2:27 PM EST Project Member

**Status:** Assigned (was: Unconfirmed)

Comment 8 by sheriffbot on Wed, Feb 16, 2022, 12:47 PM EST Project Member

**Labels:** M-98 Target-98

Setting milestone and target because of high severity.

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

Comment 9 by steimel@chromium.org on Thu, Feb 17, 2022, 11:00 AM EST Project Member

**Owner:** taku...@chromium.org
**Cc:** steimel@chromium.org

Assigning to takumif@ to triage since it looks to be related to presentation requests

Comment 10 by sheriffbot on Tue, Mar 1, 2022, 12:21 PM EST Project Member

takumif: Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

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 11 by taku...@chromium.org on Thu, Mar 3, 2022, 1:08 PM EST Project Member

**Status:** Started (was: Assigned)

I haven't been able to repro on Linux and don't have a Windows workstation that has access to two monitors.
I however have a speculative fix up at https://chromium-review.googlesource.com/c/chromium/src/+/3499791

Comment 12 by Git Watcher on Thu, Mar 3, 2022, 1:54 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4b4ba391d5ab114f2a4f06fabb307be86bf65eeb

commit 4b4ba391d5ab114f2a4f06fabb307be86bf65eeb
Author: Takumi Fujimoto <takumif@chromium.org>
Date: Thu Mar 03 18:52:55 2022

Hide media and cast dialogs before showing another

Ensure that HideDialog() gets called before creating a new dialog
instance, so that cleanup gets done.

~~Bug: 1297404~~
Change-Id: I488938c381c7327fc1999a9ef0a3872fd6053907
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499791
Reviewed-by: Tommy Steimel <steimel@chromium.org>
Reviewed-by: Muyao Xu <muyaoxu@google.com>
Commit-Queue: Takumi Fujimoto <takumif@chromium.org>
Cr-Commit-Position: refs/heads/main@{#977216}

[modify]
https://crrev.com/4b4ba391d5ab114f2a4f06fabb307be86bf65eeb/chrome/browser/ui/views/media_router/cast_dialog_view.cc
[modify]
https://crrev.com/4b4ba391d5ab114f2a4f06fabb307be86bf65eeb/chrome/browser/ui/views/global_media_controls/media_dialog_view.cc

Comment 13 by abalq...@microsoft.com on Mon, Mar 7, 2022, 2:35 AM EST

It turns out you do not need dual monitors to repro on windows.

Comment 14 by taku...@chromium.org on Mon, Mar 7, 2022, 11:59 AM EST Project Member

The speculative fix in comment 12 landed in 101.0.4923.0. Would you mind checking if it still repros on that version or later?

Comment 15 by abalq...@microsoft.com on Fri, Mar 11, 2022, 7:27 AM EST

Not able to repro on 101.0.4938.0 ASAN, did multiple runs and verified it still works on older build. So LGTM, nice patch!

Comment 16 by taku...@google.com on Fri, Mar 11, 2022, 9:48 AM EST Project Member

**Status:** Verified (was: Started)

Thank you for verifying!

Comment 17 by sheriffbot on Fri, Mar 11, 2022, 1:42 PM EST Project Member

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

Comment 18 by sheriffbot on Fri, Mar 11, 2022, 2:02 PM EST Project Member

**Labels:** Merge-Request-100 Merge-Request-98 Merge-Request-99

Requesting merge to extended stable M98 because latest trunk commit (977216) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (977216) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (977216) appears to be after beta branch point (972766).

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

Comment 19 by sheriffbot on Fri, Mar 11, 2022, 2:08 PM EST Project Member

**Labels:** -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 is already shipping to beta.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), dgagnon (ChromeOS), srinivassista (Desktop)

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

Comment 20 by sheriffbot on Fri, Mar 11, 2022, 2:08 PM EST Project Member

**Labels:** -Merge-Request-99 Merge-Review-99

Merge review required: M99 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so,

please describe required testing.

Please contact the milestone owner if you have questions.

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

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

Comment 21 by sheriffbot on Fri, Mar 11, 2022, 2:08 PM EST Project Member

**Labels:** -Merge-Request-98 Merge-Review-98

Merge review required: M98 is already shipping to stable.

Please answer the following questions so that we can safely process your merge request:
1. Why does your merge fit within the merge criteria for these milestones?
- Chrome Browser: https://chromiumdash.appspot.com/branches
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. What changes specifically would you like to merge? Please link to Gerrit.
3. Have the changes been released and tested on canary?
4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.

Please contact the milestone owner if you have questions.
Owners: govind (Android), harrysouders (iOS), matthewjoseph (ChromeOS), srinivassista (Desktop)

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

Comment 22 by srinivassista@google.com on Mon, Mar 14, 2022, 1:03 PM EDT Project Member

pls answer comment #21 for merge review.

Comment 23 by taku...@chromium.org on Mon, Mar 14, 2022, 1:27 PM EDT Project Member

1. Why does your merge fit within the merge criteria for these milestones?
High-severity security issue

2. What changes specifically would you like to merge? Please link to Gerrit.
https://chromium-review.googlesource.com/c/chromium/src/+/3499791

3. Have the changes been released and tested on canary?
Yes

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?
No

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents
N/A

6. If this merge addresses a major issue in the stable channel, does it require manual verification by the test team? If so, please describe required testing.
No

Comment 24 by srinivassista@google.com on Tue, Mar 15, 2022, 1:16 PM EDT Project Member

**Labels:** -Merge-Review-100 Merge-Approved-100

Merge approved for M100 branch: please refer to go/chrome-branches for info

Please complete your merge by 2pm PST today so it can be included in this weeks beta release.

Comment 25 by srinivassista@google.com on Tue, Mar 15, 2022, 3:39 PM EDT Project Member

CP CL here - https://chromium-review.googlesource.com/c/chromium/src/+/3526619

Please help land it

Comment 26 by Git Watcher on Tue, Mar 15, 2022, 5:06 PM EDT Project Member

**Labels:** -merge-approved-100 merge-merged-4896 merge-merged-100

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f3c85fc8e436069633e0082cb3de060a2ff8db46

commit f3c85fc8e436069633e0082cb3de060a2ff8db46
Author: Takumi Fujimoto <takumif@chromium.org>
Date: Tue Mar 15 21:05:56 2022

Hide media and cast dialogs before showing another

Ensure that HideDialog() gets called before creating a new dialog
instance, so that cleanup gets done.

(cherry picked from commit 4b4ba391d5ab114f2a4f06fabb307be86bf65eeb)

~~Bug: 1297404~~
Change-Id: I488938c381c7327fc1999a9ef0a3872fd6053907
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499791
Reviewed-by: Tommy Steimel <steimel@chromium.org>
Reviewed-by: Muyao Xu <muyaoxu@google.com>
Commit-Queue: Takumi Fujimoto <takumif@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977216}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3526619
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Reviewed-by: Takumi Fujimoto <takumif@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#572}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/f3c85fc8e436069633e0082cb3de060a2ff8db46/chrome/browser/ui/views/media_router/cast_dialog_view.cc
[modify]
https://crrev.com/f3c85fc8e436069633e0082cb3de060a2ff8db46/chrome/browser/ui/views/global_media_controls/media_dialog_view.cc

Comment 27 by sheriffbot on Tue, Mar 15, 2022, 5:10 PM EDT Project Member

**Labels:** LTS-Merge-Candidate

LTS Milestone M96

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle

This issue has been flagged as a merge candidate for Chrome OS' LTS channel. If selected, our merge team will handle any additional merges. To help us determine if this issue requires a merge to LTS, please answer this short questionnaire:
1. Was this issue a regression for the milestone it was found in?
2. Is this issue related to a change or feature merged after the latest LTS Milestone?

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

Comment 28 by rzanoni@google.com on Wed, Mar 16, 2022, 5:09 AM EDT Project Member

**Cc:** rzanoni@google.com
**Labels:** LTS-Evaluating-96

Comment 29 by rzanoni@google.com on Thu, Mar 17, 2022, 8:55 AM EDT Project Member

**Labels:** -LTS-Evaluating-96 LTS-Merge-Request-96

Comment 30 by sheriffbot on Thu, Mar 17, 2022, 8:59 AM EDT Project Member

**Labels:** -LTS-Merge-Request-96 LTS-Merge-Review-96

This issue requires additional review before it can be merged to the LTS channel. Please answer the following questions to help us evaluate this merge:

1. Number of CLs needed for this fix and links to them.
2. Level of complexity (High, Medium, Low - Explain)
3. Has this been merged to a stable release? beta release?
4. Overall Recommendation (Yes, No)

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

Comment 31 by rzanoni@google.com on Thu, Mar 17, 2022, 9:03 AM EDT Project Member

1. Just https://crrev.com/c/3528415
2. Low, mostly conflicts missing methods in M96, simple to solve
3. 100
4. Yes

Comment 32 by gmpritchard@google.com on Thu, Mar 17, 2022, 10:42 AM EDT Project Member

**Labels:** LTS-Merge-Delayed-96

Delaying merge approval until it gets pushed on beta.

Comment 33 by amyressler@chromium.org on Thu, Mar 17, 2022, 1:05 PM EDT Project Member

**Labels:** -Merge-Review-98 -Merge-Review-99

no further planned releases of M99 stable or M98 extended stable

Comment 34 by gmpritchard@google.com on Fri, Mar 25, 2022, 9:43 AM EDT Project Member

**Labels:** -LTS-Merge-Candidate -LTS-Merge-Delayed-96 LTS-Merge-Approved-96

Comment 35 by Git Watcher on Sun, Mar 27, 2022, 9:11 PM EDT Project Member

**Labels:** merge-merged-4664

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f2fdce105c82fb6b860309d0f0d49d65b3a24979

commit f2fdce105c82fb6b860309d0f0d49d65b3a24979
Author: Takumi Fujimoto <takumif@chromium.org>
Date: Mon Mar 28 01:10:10 2022

[M96-LTS] Hide media and cast dialogs before showing another

M96 merge issues:
media_dialog_view.cc:
- conflicting declarations of MediaDialogView constructor
cast_dialog_view.cc:
ShowAccessCodeCastDialog() and MaybeShowAccessCodeCastButton()
not present in M96

Ensure that HideDialog() gets called before creating a new dialog
instance, so that cleanup gets done.

(cherry picked from commit 4b4ba391d5ab114f2a4f06fabb307be86bf65eeb)

~~Bug: 1297404~~
Change-Id: I488938c381c7327fc1999a9ef0a3872fd6053907
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499791
Commit-Queue: Takumi Fujimoto <takumif@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#977216}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3528415
Reviewed-by: Oleh Lamzin <lamzin@google.com>
Owners-Override: Oleh Lamzin <lamzin@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4664@{#1553}
Cr-Branched-From: 24dc4ee75e01a29d390d43c9c264372a169273a7-refs/heads/main@{#929512}

[modify]
https://crrev.com/f2fdce105c82fb6b860309d0f0d49d65b3a24979/chrome/browser/ui/views/media_router/cast_dialog_view.cc
[modify]
https://crrev.com/f2fdce105c82fb6b860309d0f0d49d65b3a24979/chrome/browser/ui/views/global_media_controls/media_dialog_view.cc

Comment 36 by rzanoni@google.com on Mon, Mar 28, 2022, 5:32 AM EDT Project Member

**Labels:** -LTS-Merge-Approved-96 -LTS-Merge-Review-96 LTS-Merge-Merged-96

Comment 37 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:55 PM EDT Project Member

**Labels:** Release-0-M100

Comment 38 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

**Labels:** CVE-2022-1131 CVE_description-missing

Comment 39 by sheriffbot on Fri, Jun 17, 2022, 1:31 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 40 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

**Labels:** CVE_description-submitted -CVE_description-missing

Comment 41 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

**Labels:** -CVE_description-missing --CVE_description-missing