Starred by 3 users

Owner:	liber...@chromium.org
CC:	boliu@chromium.org bartekn@chromium.org creis@chromium.org mcnee@chromium.org steimel@chromium.org haraken@chromium.org dcheng@chromium.org rsch...@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Layout Internals>Media
Modified:	Jul 21, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Android
Pri:	0
Type:	Bug-Security

Hotlist-Merge-Review
Security_Severity-Critical
Hotlist-Merge-Approved
allpublic
CVE_description-submitted
M-98
Target-98
FoundIn-96
Security_Impact-Extended
merge-merged-4758
merge-merged-98
merge-merged-4844
merge-merged-99
merge-merged-4896
merge-merged-100
Release-1-M99
CVE-2022-0971

Issue 1299422: Security: heap-use-after-free in content::DisplayCutoutHostImpl::SendSafeAreaToFrame

Reported by glazunov@google.com on Mon, Feb 21, 2022, 8:56 AM EST Project Member

Code

SUMMARY
A use-after-free issue exists in Chrome 100 and earlier versions. Processing maliciously crafted web content may lead to arbitrary code execution in the browser process.

VULNERABILITY DETAILS

```
void DisplayCutoutHostImpl::DidFinishNavigation(
    NavigationHandle* navigation_handle) {
  // If the navigation is not in the main frame or if we are a same document
  // navigation then we should stop now.
  if (!navigation_handle->IsInPrimaryMainFrame() ||
      navigation_handle->IsSameDocument()) {
    return;
  }

  // If we finish a main frame navigation and the |WebDisplayMode| is
  // fullscreen then we should make the main frame the current
  // |RenderFrameHost|.
  blink::mojom::DisplayMode mode = web_contents_impl_->GetDisplayMode();
  if (mode == blink::mojom::DisplayMode::kFullscreen)
    SetCurrentRenderFrameHost(web_contents_impl_->GetMainFrame());
}

void DisplayCutoutHostImpl::RenderFrameDeleted(RenderFrameHost* rfh) {
  values_.erase(rfh);

  // If we were the current |RenderFrameHost| then we should clear that.
  if (current_rfh_ == rfh)
    SetCurrentRenderFrameHost(nullptr);
}

void DisplayCutoutHostImpl::SetCurrentRenderFrameHost(RenderFrameHost* rfh) {
  if (current_rfh_ == rfh)
    return;

  // If we had a previous frame then we should clear the insets on that frame.
  if (current_rfh_)
    SendSafeAreaToFrame(current_rfh_, gfx::Insets());

  // Update the |current_rfh_| with the new frame.
  current_rfh_ = rfh;

[...]
}
```

This is yet another issue caused by the error-prone frame state tracking design that has been discussed in ~~https://crbug.com/1260007~~.

`DisplayCutoutHostImpl` subscribes to `RenderFrameDeleted` notifications so that it can clear the raw pointer field `current_rfh_` when the frame host gets destroyed. Unfortunately, the `DidFinishNavigation` method, which sets the pointer, may be called after the frame host has been put into the "deleted" (meaning `RenderFrameDeleted` has been called) state, for example, if the associated renderer process crashes before the navigation can complete. Since `RenderFrameDeleted` can't be called twice on the same object, `DisplayCutoutHostImpl` won't be notified, and `current_rfh_` will be left dangling.

`SetCurrentRenderFrameHost` should be modified to check whether the new frame host is alive to fix the issue.

VERSION
Note that `DisplayCutoutHostImpl` is only enabled for Android, so other OSes are not affected.

Google Chrome 98.0.4758.101 (Official Build) (64-bit)
100.0.4893.0 (Developer Build) (64-bit)

REPRODUCTION CASE
1. Apply the attached patch to enable `DisplayCutoutHostImpl` for Linux.
2. Run the custom web server script.
3. Start Chrome: `/path/to/chrome --js-flags="--allow-natives-syntax" http://localhost:8000/repro.html`. The repro case calls a V8 native function to crash the renderer. Of course, any other way would work as well.

CREDIT INFORMATION
Sergei Glazunov of Google Project Zero

asan.log
28.7 KB View Download

patch.diff
751 bytes View Download

repro.html
740 bytes View Download

server.py
411 bytes View Download

Comment 1 by glazunov@google.com on Mon, Feb 21, 2022, 8:59 AM EST Project Member

Cc: dcheng@chromium.org

Comment 2 by danakj@chromium.org on Tue, Feb 22, 2022, 5:59 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: dalec...@chromium.org
Cc: creis@chromium.org mcnee@chromium.org
Labels: Security_Severity-Critical OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-iOS OS-Lacros Pri-1
Components: Internals>Media

dalecurtis@ could you please triage?

It seems the authors of this class no longer work here.
And the OWNERS file here, and in a couple other places, points to a 404.

https://source.chromium.org/search?ss=chromium%2Fchromium%2Fsrc&q=chrome%2Fandroid%2Fjava%2Fsrc%2Forg%2Fchromium%2Fchrome%2Fbrowser%2Fdisplay_cutout%2FOWNERS

In general: outliving a document and tracking the RenderFrameHost* is very problematic. Using a raw pointer is extra bad: https://docs.google.com/document/d/1oopBPfX88thk6Ax79h_UbaoNQt416t7iNjrF38veuSg/edit?resourcekey=0-A4afoyISzgiyd667or1Xmw

If a class wants to outlive a document it should track the FrameTreeNode (or WebContents) rather than the RenderFrameHost.

Comment 3 by danakj@chromium.org on Tue, Feb 22, 2022, 6:00 PM EST Project Member

Labels: FoundIn-96

All the code here is > 1 year old so would be in M96 .

Comment 4 by sheriffbot on Tue, Feb 22, 2022, 6:05 PM EST Project Member

Labels: Security_Impact-Extended

Comment 5 by dalec...@chromium.org on Tue, Feb 22, 2022, 6:12 PM EST Project Member

Owner: liber...@chromium.org
Cc: steimel@chromium.org

=>Frank to triage since this was previously owned by Chrome Media UX (beccahughes@, mlamouri@)

Comment 6 by liberato@google.com on Tue, Feb 22, 2022, 6:31 PM EST Project Member

Status: Started (was: Assigned)

this looks like more fun than perf. putting together a CL now.

Comment 7 by dcheng@chromium.org on Tue, Feb 22, 2022, 8:52 PM EST Project Member

Status: Assigned (was: Started)
Owner: dalec...@chromium.org
Components: Blink>Layout

I've filed issue 1300030 since this component does not appear to have any active OWNERS.

We did cover this implementation class in a previous audit; however, we made the incorrect assumption that

We did cover this implementation class in a previous audit; however, we made the incorrect assumption that DidFinishNavigation() is not called after RenderFrameDeleted().

In general, this is a super error prone way of handling lifetimes: we don't provide any easy way to automatically scope lifetimes, so code ends up having to listen for these notifications.

+dalecurtis, can you help find an OWNER for this? I guess this is ostensibly a 'media' feature, though I don't really know who works in this area anymore: mlamouri and beccahughes were the only two OWNERS, and both have moved off Chrome. The short-term fix (to simply add a liveness check) should be easy to implement.

Critical, because this does not require a compromised renderer to trigger the memory corruption.
Blink>Layout because that's what the only DIR_METADATA I could find claims.

Comment 8 by dcheng@chromium.org on Tue, Feb 22, 2022, 8:53 PM EST Project Member

Status: Started (was: Assigned)
Owner: liber...@chromium.org
Labels: -OS-Linux -OS-Windows -OS-iOS -OS-Chrome -OS-Mac -OS-Fuchsia -OS-Lacros

Oh, I should have refreshed. Fixing OWNERS assignment.

(I am removing the OS labels except for Android though; this is only reachable on Android)

Comment 9 by liberato@google.com on Wed, Feb 23, 2022, 12:57 AM EST Project Member

https://chromium-review.googlesource.com/c/chromium/src/+/3482540

Comment 10 by liberato@google.com on Wed, Feb 23, 2022, 12:58 AM EST Project Member

also, thank you for the detailed repro steps.

Comment 11 by sheriffbot on Thu, Feb 24, 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 12 by sheriffbot on Thu, Feb 24, 2022, 1:13 PM EST Project Member

Labels: -Pri-1 Pri-0

Setting Pri-0 to match security severity Critical. 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 13 by creis@chromium.org on Tue, Mar 1, 2022, 11:39 AM EST Project Member

Cc: boliu@chromium.org

liberato@ / danakj@ / dcheng@ / boliu@: What's the status of this? Can we unblock the CL and get it landed, given the critical severity rating? Thanks!

Comment 14 by liberato@google.com on Tue, Mar 1, 2022, 12:01 PM EST Project Member

the CL [1] is coming along.

[1] https://chromium-review.googlesource.com/c/chromium/src/+/3482540

[1] https://chromium-review.googlesource.com/c/chromium/src/+/3482540

Comment 15 by Git Watcher on Tue, Mar 1, 2022, 3:03 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/4d71d571302a75192f26d9e1122150ae5c600abb

commit 4d71d571302a75192f26d9e1122150ae5c600abb
Author: liberato@chromium.org <liberato@chromium.org>
Date: Tue Mar 01 20:02:12 2022

Don't use a deleted RenderFrameHost.

Since we do not check for frame liveness, a RenderFrameHost might be
deleted (in the use-after-free sense) without another call to
RenderFrameDeleted. So, WeakPtr it to avoid these cases.

~~Bug: 1299422~~
Change-Id: Ie4fe85f88ef80f4e4c3d0452397c0e5050ed881c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482540
Reviewed-by: Bo Liu <boliu@chromium.org>
Commit-Queue: Frank Liberato <liberato@chromium.org>
Auto-Submit: Frank Liberato <liberato@chromium.org>
Cr-Commit-Position: refs/heads/main@{#976357}

[modify]
https://crrev.com/4d71d571302a75192f26d9e1122150ae5c600abb/content/browser/display_cutout/display_cutout_host_impl.h
[modify]
https://crrev.com/4d71d571302a75192f26d9e1122150ae5c600abb/content/browser/display_cutout/display_cutout_host_impl.cc

Comment 16 by liberato@google.com on Tue, Mar 1, 2022, 7:34 PM EST Project Member

Status: Fixed (was: Started)

Comment 17 by sheriffbot on Wed, Mar 2, 2022, 1:41 PM EST Project Member

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

Comment 18 by sheriffbot on Wed, Mar 2, 2022, 2:01 PM EST Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (976357) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (976357) appears to be after stable branch point (961656).

Requesting merge to dev M100 because latest trunk commit (976357) appears to be after dev branch point (972766).

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

Comment 19 by sheriffbot on Wed, Mar 2, 2022, 3:04 PM EST Project Member

Labels: -Merge-Request-100 Merge-Approved-100 Hotlist-Merge-Approved

Merge approved: your change passed merge requirements and is auto-approved for M100. Please go ahead and merge the CL to branch 4896 (refs/branch-heads/4896) manually. Please contact milestone owner if you have questions.
Merge instructions:
https://chromium.googlesource.com/chromium/src.git/+/refs/heads/main/docs/process/merge_request.md
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 Wed, Mar 2, 2022, 3:04 PM EST Project Member

Labels: -Merge-Request-99 Hotlist-Merge-Review 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.
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 Wed, Mar 2, 2022, 3:04 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 liberato@google.com on Wed, Mar 2, 2022, 3:53 PM EST Project Member

re c#19: cherry-pick to M100 is at https://chromium-review.googlesource.com/c/chromium/src/+/3498952

Comment 23 by sheriffbot on Mon, Mar 7, 2022, 12:22 PM EST 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 24 by amyressler@chromium.org on Mon, Mar 7, 2022, 12:58 PM EST Project Member

Labels: -Merge-Review-98 -Merge-Review-99 Merge-Approved-99 Merge-Approved-98

M99 merge approved, please merge to branch 4844 before noon PST, Thursday, 10 March so this fix can be included in the next stable security refresh
M98 merge approved, please merge to branch 4758 so this fix can be included in Extended stable support

Comment 25 by liberato@google.com on Mon, Mar 7, 2022, 1:35 PM EST Project Member

M99: https://chromium-review.googlesource.com/c/chromium/src/+/3508293
M98: https://chromium-review.googlesource.com/c/chromium/src/+/3508294

Comment 26 by Git Watcher on Mon, Mar 7, 2022, 3:14 PM EST Project Member

Labels: -merge-approved-98 merge-merged-4758 merge-merged-98

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/cebad8ef22dc7b07430fed392518726a62bd25d4

commit cebad8ef22dc7b07430fed392518726a62bd25d4
Author: liberato@chromium.org <liberato@chromium.org>
Date: Mon Mar 07 20:13:16 2022

[M98] Don't use a deleted RenderFrameHost.

Since we do not check for frame liveness, a RenderFrameHost might be
deleted (in the use-after-free sense) without another call to
RenderFrameDeleted. So, WeakPtr it to avoid these cases.

(cherry picked from commit 4d71d571302a75192f26d9e1122150ae5c600abb)

~~Bug: 1299422~~
Change-Id: Ie4fe85f88ef80f4e4c3d0452397c0e5050ed881c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482540
Reviewed-by: Bo Liu <boliu@chromium.org>
Commit-Queue: Frank Liberato <liberato@chromium.org>
Auto-Submit: Frank Liberato <liberato@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#976357}

Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508294
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Bo Liu <boliu@chromium.org>

Commit-Queue: Bo Liu <boliu@chromium.org>
Cr-Commit-Position: refs/branch-heads/4758@{#1232}
Cr-Branched-From: 4a2cf4baf90326df19c3ee70ff987960d59a386e-refs/heads/main@{#950365}

[modify]
https://crrev.com/cebad8ef22dc7b07430fed392518726a62bd25d4/content/browser/display_cutout/display_cutout_host_impl.h
[modify]
https://crrev.com/cebad8ef22dc7b07430fed392518726a62bd25d4/content/browser/display_cutout/display_cutout_host_impl.cc

Comment 27 by Git Watcher on Mon, Mar 7, 2022, 3:18 PM EST Project Member

Labels: -merge-approved-99 merge-merged-4844 merge-merged-99

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e3e7862718bce4eb785c59d96359a35ca64c6ac5

commit e3e7862718bce4eb785c59d96359a35ca64c6ac5
Author: liberato@chromium.org <liberato@chromium.org>
Date: Mon Mar 07 20:17:13 2022

[M99] Don't use a deleted RenderFrameHost.

Since we do not check for frame liveness, a RenderFrameHost might be
deleted (in the use-after-free sense) without another call to
RenderFrameDeleted. So, WeakPtr it to avoid these cases.

(cherry picked from commit 4d71d571302a75192f26d9e1122150ae5c600abb)

~~Bug: 1299422~~
Change-Id: Ie4fe85f88ef80f4e4c3d0452397c0e5050ed881c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482540
Reviewed-by: Bo Liu <boliu@chromium.org>
Commit-Queue: Frank Liberato <liberato@chromium.org>
Auto-Submit: Frank Liberato <liberato@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#976357}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3508293
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Bo Liu <boliu@chromium.org>
Cr-Commit-Position: refs/branch-heads/4844@{#997}
Cr-Branched-From: 007241ce2e6c8e5a7b306cc36c730cd07cd38825-refs/heads/main@{#961656}

[modify]
https://crrev.com/e3e7862718bce4eb785c59d96359a35ca64c6ac5/content/browser/display_cutout/display_cutout_host_impl.h
[modify]
https://crrev.com/e3e7862718bce4eb785c59d96359a35ca64c6ac5/content/browser/display_cutout/display_cutout_host_impl.cc

Comment 28 by eakpobaro@google.com on Tue, Mar 8, 2022, 9:38 AM EST Project Member

[Bulk edit]

This has been approved for merge, please merge ASAP

This has been approved for merge , please merge ASAP

Comment 29 by Git Watcher on Tue, Mar 8, 2022, 5:56 PM EST 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/+/db880005f1f0b17ee1702629c225a8044ccc9d3b

commit db880005f1f0b17ee1702629c225a8044ccc9d3b
Author: liberato@chromium.org <liberato@chromium.org>
Date: Tue Mar 08 22:55:06 2022

[M100] Don't use a deleted RenderFrameHost.

Since we do not check for frame liveness, a RenderFrameHost might be
deleted (in the use-after-free sense) without another call to
RenderFrameDeleted. So, WeakPtr it to avoid these cases.

(cherry picked from commit 4d71d571302a75192f26d9e1122150ae5c600abb)

~~Bug: 1299422~~
Change-Id: Ie4fe85f88ef80f4e4c3d0452397c0e5050ed881c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482540
Reviewed-by: Bo Liu <boliu@chromium.org>
Commit-Queue: Frank Liberato <liberato@chromium.org>
Auto-Submit: Frank Liberato <liberato@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#976357}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3498952
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4896@{#398}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/db880005f1f0b17ee1702629c225a8044ccc9d3b/content/browser/display_cutout/display_cutout_host_impl.h
[modify]
https://crrev.com/db880005f1f0b17ee1702629c225a8044ccc9d3b/content/browser/display_cutout/display_cutout_host_impl.cc

Comment 30 by amyressler@chromium.org on Fri, Mar 11, 2022, 3:24 PM EST Project Member

Labels: Release-1-M99

Comment 31 by amyressler@google.com on Mon, Mar 14, 2022, 6:13 PM EDT Project Member

Labels: CVE-2022-0971 CVE_description-missing

Comment 32 by adetaylor@google.com on Tue, Mar 15, 2022, 2:46 PM EDT Project Member

Cc: rsch...@chromium.org

Comment 33 by sheriffbot on Wed, Jun 8, 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.

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 34 by lukasza@chromium.org on Thu, Jun 30, 2022, 10:47 AM EDT Project Member

Cc: haraken@chromium.org bartekn@chromium.org

Comment 35 by amyressler@google.com on Thu, Jul 21, 2022, 5:06 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 36 by amyressler@chromium.org on Thu, Jul 21, 2022, 6:13 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing