Starred by 3 users

Owner: michaelludwig@google.com

CC: sunn...@chromium.org
michaelludwig@google.com
pdr@chromium.org
bsalomon@chromium.org
adetaylor@chromium.org
ikilpatrick@chromium.org
kylec...@chromium.org
mcasas@chromium.org

Status: Fixed *(Closed)*

Components: Internals>GPU>Video
Internals>Compositing

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: 2022-03-14

OS: Linux, Windows

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
reward-3000
Arch-x86_64
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
FoundIn-89
external_security_report
M-98
Target-98
Security_Impact-Extended
merge-merged-4896
merge-merged-100
Release-2-M100
CVE-2022-1306

Issue 1299287: Video escapes content area

Reported by xpsve...@gmail.com on Sun, Feb 20, 2022, 3:57 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.88 Safari/537.36

Steps to reproduce the problem:
1. Extract PoC.zip to a folder. Open PoC.html.
2. Scroll down the page.
3. If the security bug doesn't trigger, scroll all the way back up to the top and repeat step 2.

Sometimes easier to reproduce in maximized chromium/chrome

What is the expected behavior?
UI is not overlayed by large video tag.

What went wrong?
UI is overlayed with video element. This could be used for UI spoofing.

Did this work before? Yes I think this regressed a long time ago

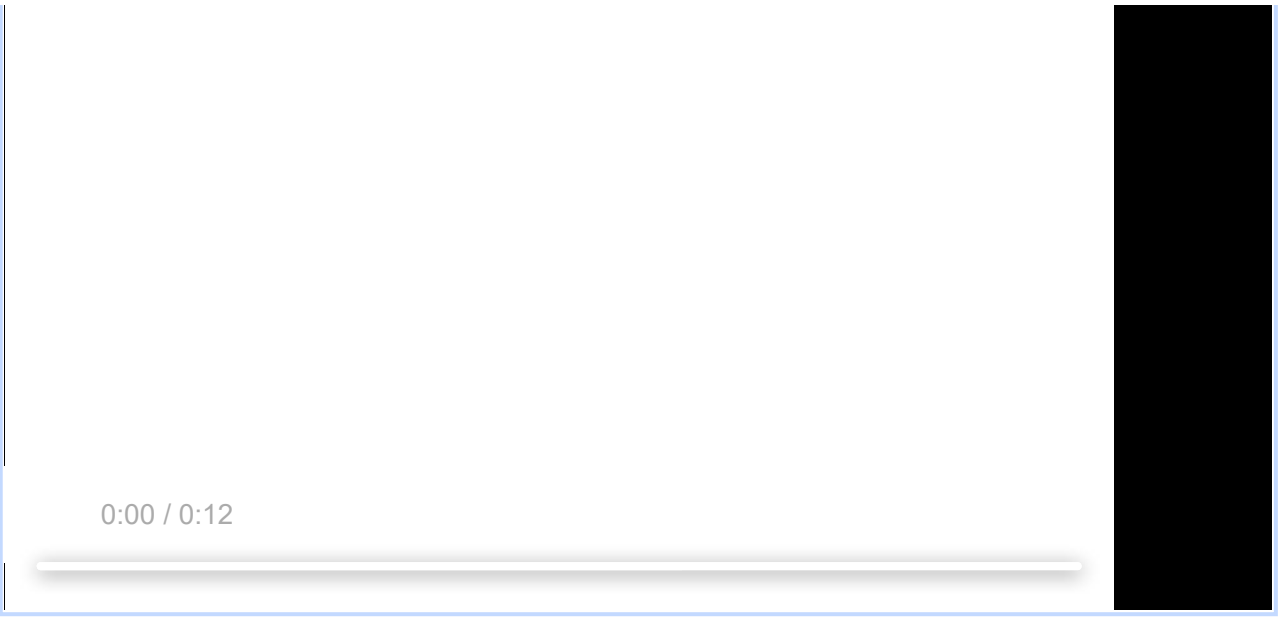
Chrome version: 101.0.4899.0 Channel: canary
OS Version: 11

The UI comes back when you hover your mouse over the native UI elements, I.E. address bar, tab bar, etc...

Other browsers like Vivaldi, Edge and Brave (in some scenarios) have worse symptoms than Chrome/Chromium such as the UI staying overlayed even when you hover your mouse over the native UI.

PoC.zip
19.8 KB Download

chrome_i2G6SFEl99.mp4
475 KB View Download



Comment 1 by sheriffbot on Sun, Feb 20, 2022, 4:01 PM EST Project Member

Labels: external_security_report

Comment 2 by danakj@chromium.org on Wed, Feb 23, 2022, 12:25 PM EST Project Member

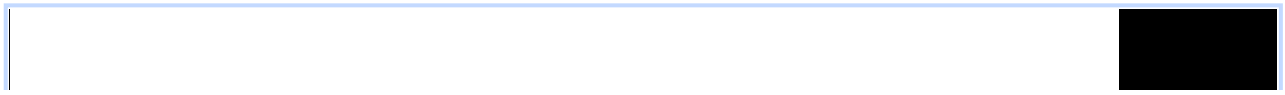
Summary: Video escapes content area (was: Video tags with a huge height overlaps Chromium UI)
Status: Assigned (was: Unconfirmed)
Owner: sunn...@chromium.org
Labels: Security_Severity-High Pri-1
Components: Internals>GPU>Video Internals>Compositing

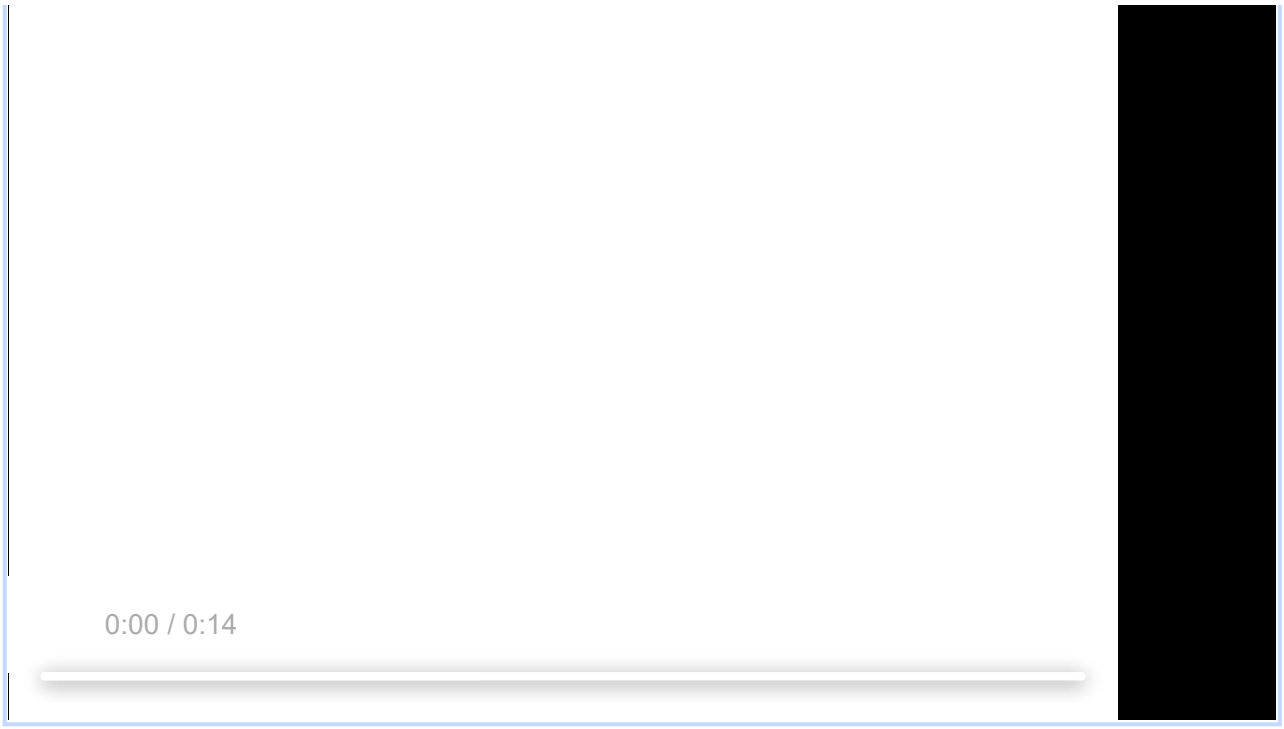
I could not repro on Linux but given the nature this is likely a Windows-specific compositing path. I don't have a WIndows machine to repro and Clusterfuzz won't help here, so => OWNERS

Comment 3 by xpsve...@gmail.com on Wed, Feb 23, 2022, 12:47 PM EST

I can reproduce this issue on Ubuntu 21.10 100.0.4867.0 (Official Build) dev (64-bit).

ubuntu_video_height.mp4
264 KB View Download





Comment 4 by sunn...@chromium.org on Thu, Feb 24, 2022, 1:24 PM EST Project Member

Cc: adetaylor@chromium.org

I can reproduce this on my Windows workstation, and observed the following:
--disable-gpu fixes it
--disable-direct-composition has no effect
SW video decoder is being used
Scrolling with mouse or keyboard triggers it, but scrolling with scrollbar doesn't

I suspect something's off with either the bounds or damage rect in cc/viz due to the abnormally large height on the video element.

I'm not sure about the severity of the bug - it seems you wanted to spoof the address bar with the video you provided, but you had to set a really large height on the video element to get it to obscure the address bar and that causes the video to stretch out a lot showing only a grey block over the address bar which surely can't be mistaken for the real address bar. It would be far more interesting if you could spoof the address bar in a believable manner.

Comment 5 by xpsve...@gmail.com on Thu, Feb 24, 2022, 2:27 PM EST

Thank you for investigating. The video was meant to be unrelated in my PoC. I apologize if that created any confusion.

The reason the spoof isn't convincing right now, and you mentioned it, is because the video is stretched out with "object-fill: fill" while having small dimensions. Theoretically you could create a video that has a height of 99999999px+ and set the top of that video to a static image of whatever you wanted to spoof. It then could be spoofed.

I do not currently have the tools to create such a video, but I will see what I can do.

Comment 6 by sunn...@chromium.org on Thu, Feb 24, 2022, 6:40 PM EST Project Member

Cc: a_deleted_user ikilpatrick@chromium.org kylec...@chromium.org

Here's what I get when I log the transform and pre-transform visible rect for the video quad as seen by SkiaRenderer:

[10356:53216:0224/153429.392:INFO:skia_renderer.cc(1840)] content_device_transform = [+1.1710, +0.0000, +0.0000

[19356:53216:0224/153429.392:INFO:skia_renderer.cc(1840)] content_device_transform = [+1.1719 +0.0000 +0.0000
+0.0000

+0.0000 +699050.5625 +0.0000 -10693.0000
+0.0000 +0.0000 +1.0000 +0.0000
+0.0000 +0.0000 +0.0000 +1.0000]

[19356:53216:0224/153429.393:INFO:skia_renderer.cc(1644)] visible_rect = 0,0.0154495 2560x0.00284958

We set the transform on the SkCanvas and use the visible rect in the ImageSetEntry. So Skia is going to end up multiplying a very small height (in the pre-transform space) with a very large scale factor which could easily overflow and then be clipped to the entire screen.

kylechar: Do you think it's feasible to apply a scissor rect to quads based on the bounds of the surface they were contained in pre-aggregation? We currently only use scissor rect to limit to the render pass surface size. Any other ideas on how to mitigate this in viz?

masonfreed, ikilpatrick: I suspect the page uses LayoutReplaced for the video element given the "object-fill: fill". Should there be protections against this kind of overflow in blink, or should we do something about this in viz?

Comment 7 by ikilpatrick@chromium.org on Thu, Feb 24, 2022, 6:47 PM EST Project Member

Cc: pdr@chromium.org

pdr@ might be in a better position to answer the question related to the visible rect of the element.

Comment 8 by pdr@chromium.org on Thu, Feb 24, 2022, 6:56 PM EST Project Member

Sunny, is this specific to video? It should be possible to add all sorts of extreme transforms on content in general, since it will be clipped by the viewport.

It may be worth bisecting this to see if it is a recent regression. That will at least point to likely places to investigate.

Comment 9 by kylec...@chromium.org on Mon, Feb 28, 2022, 10:05 AM EST Project Member

Cc: michaelludwig@google.com bsalomon@chromium.org

> kylechar: Do you think it's feasible to apply a scissor rect to quads based on the bounds of the surface they were contained in pre-aggregation? We currently only use scissor rect to limit to the render pass surface size.

I think we already do this? We clip based on the bounds of the SurfaceDrawQuad. There's two cases for drawing an embedded surface content, either the child surfaces root render pass is drawn to it's own texture or merged into the embedding RP. If the child root RP is drawn to it's own texture first then that texture has the visible_rect+clip_rect of the SurfaceDrawQuad applied when it's drawn to the embedding RP. If the child root RP is merged into the embedding RP then the visible_rect+clip_rect from the SurfaceDrawQuad is added to |surface_quad_clip| [1]. |surface_quad_clip| is passed to CopyQuadsToPass() and then added to every DrawQuad from the child root RP. SkiaRenderer uses the SQS::clip_rect to scissor/clip internally with optimizations to avoid unnecessary clipping.

It's possible there is a bug in the clip_rect calculations in SurfaceAggregator/DirectRenderer but that seems like it should impact SoftwareRenderer too.

It's also possible that huge transform is tripping up Skia (numerical instability?) so that it's not correctly applying clip/scissor. Something similar happened with large perspective transforms in ~~issue 1272250~~.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:components/viz/service/display/surface_aggregator.cc;l=808;

drc=c415e972fa4afd284ebc398aabea3a19da9b1128

Comment 10 by michaelludwig@google.com on Mon, Feb 28, 2022, 12:11 PM EST Project Member

This does sound similar to ~~issue 1272250~~. In 1272250 the bug was in skia_renderer running into numerical stability when it tried to modify the visible rect in local space based on the device-space scissor rect. The fix should mean that skia_renderer is not doing that here. If we even make it to [1], we should detect numerical instability and not try and explicitly apply the scissor, or we should be fine and applying it won't lead to popping over the UI bar (assuming there isn't a bug in that logic of course :)). There was another issue dealing with subpixel quads (~~issue 1210170~~), and that fix may also come into play based on the logged visible_rect [2].

In either case, this should mean that skia_renderer is relying on a call to SkCanvas::clipRect() to scissor the quad. You can inspect that value at [3] to see if it looks reasonable. If that clip rect suggests the quad should not draw over the UI address bar, then there's likely a bug inside skia applying the clip rect. However, if the clip rect is not excluding the address bar, then it could be the SurfaceAggregator/DirectRenderer as Kyle suggested.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:components/viz/service/display/skia_renderer.cc;drc=7b7aaecca4adc6d0e8f87779d17774858896d02e;l=1423
[2]
https://source.chromium.org/chromium/chromium/src/+/main:components/viz/service/display/skia_renderer.cc;drc=7b7aaecca4adc6d0e8f87779d17774858896d02e;l=1410
[3]
https://source.chromium.org/chromium/chromium/src/+/main:components/viz/service/display/skia_renderer.cc;drc=0e24535efdfbc5c4adf8f10284e66d50e14a037a;l=1063

Comment 11 by ajgo@google.com on Tue, Mar 8, 2022, 5:45 PM EST Project Member

Labels: OS-Linux

adding poc as attachment

Code_-_Insiders_mSfUtYR5tL.mp4
22.7 KB View Download

PoC.html
345 bytes View Download

Comment 12 by sunn...@chromium.org on Tue, Mar 8, 2022, 5:48 PM EST Project Member

NextAction: 2022-03-14

I don't have the cycles to look into it this week - I might have some time next week though. Security team, if you feel this is time sensitive, can you please find another owner?

Comment 13 by ajgo@google.com on Tue, Mar 8, 2022, 6:11 PM EST Project Member

Labels: Found-89

bisecting a little:

vpython3 bisect_builds.py -o -a win64 -g 70.0.3538.124 -b 96.0.4664.174 D:\pocs\1299287\PoC.html

Bisecting range [803241 (good), 803243 (bad)].
Trying revision 803242...
Revision 803242 is [(g)ood/(b)ad/(r)etry/(u)nknown/(s)tdout/(q)uit]: g

Revision 803242 is [(g)ood/(b)ad/(r)etry/(u)nknown/(s)tdout/(q)uit]: g
You are probably looking for a change made after 803242 (known good), but no later than 803243 (first known bad).
CHANGELOG URL:
The script might not always return single CL as suspect as some perf builds might get missing due to failure.

https://chromium.googlesource.com/chromium/src/+log/a857108e4452b0dc2254df29a87befe8af408fdf..60789cdca25a8eb8534d0c5fccfb87c04c0f66d3

Comment 14 by ajgo@google.com on Tue, Mar 8, 2022, 6:11 PM EST Project Member

Labels: -Found-89 FoundIn-89

Comment 15 by ajgo@google.com on Tue, Mar 8, 2022, 6:12 PM EST Project Member

kylechar - seems to be directly related to enabling skia renderer.

Comment 16 by sunn...@chromium.org on Tue, Mar 8, 2022, 6:15 PM EST Project Member

Owner: kylec...@chromium.org
Cc: sunn...@chromium.org

Kyle, can you please investigate this further for now? I can take over next week if you're busy.

Comment 17 by sheriffbot on Tue, Mar 8, 2022, 6:17 PM EST Project Member

Labels: Security_Impact-Extended

Comment 18 by kylec...@chromium.org on Wed, Mar 9, 2022, 12:04 PM EST Project Member

Owner: michaelludwig@google.com

I can reproduce on Linux at ToT. I can see |clip_rect| being set on renderer quads and SkiaRenderer::scissor_rect_ being set with the same value, so we are passing through the scissor information to Skia.

The issue is likely inside Skia. michaelludwig@ can you take a look or triage?

Comment 19 by sheriffbot on Wed, Mar 9, 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 20 by michaelludwig@google.com on Thu, Mar 10, 2022, 4:55 PM EST Project Member

Have a fix at https://chromium-review.googlesource.com/c/chromium/src/+/3516507, confirmed to solve issue by Kyle. Unfortunately it has layout tests and gold test differences (acceptable), so I'm not sure how this would affect any merging.

Comment 21 by monor...@bugs.chromium.org on Mon, Mar 14, 2022, 8:00 AM EDT

The NextAction date has arrived: 2022-03-14

Comment 22 by michaelludwig@google.com on Wed, Mar 16, 2022, 2:16 PM EDT Project Member

Blockedon: skia:10456

Comment 23 by Git Watcher on Thu, Mar 17, 2022, 4:49 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/540e2ecde447b0757dd5bb079a59d8faef3183c1

commit 540e2ecde447b0757dd5bb079a59d8faef3183c1
Author: Michael Ludwig <michaelludwig@google.com>
Date: Thu Mar 17 20:48:32 2022

[skia_renderer]: Use RectF::Intersect in ApplyScissor

~~Bug: 1299287~~, ~~1307317~~
Change-Id: I026090466ebfb3dee0e9daf0609f04babcf42092
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3516507
Reviewed-by: Kyle Charbonneau <kylechar@chromium.org>
Reviewed-by: Brian Sheedy <bsheedy@chromium.org>
Commit-Queue: Michael Ludwig <michaelludwig@google.com>
Cr-Commit-Position: refs/heads/main@{#982400}

[add]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/linux/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[add]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/linux/compositing/visibility/visibility-simple-video-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/win/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/content/test/gpu/gpu_tests/test_expectations/pixel_expectations.txt
[add]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/linux/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/win/images/yuv-decode-eligible/color-profile-layer-expected.png
[add]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/linux/virtual/threaded/compositing/visibility/visibility-simple-video-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/mac/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/mac/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify] https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/flag-specific/highdpi/compositing/geometry/video-fixed-scrolling-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/flag-specific/skia-vulkan-swiftshader/compositing/visibility/visibility-simple-video-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/mac/compositing/vi

https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/mac/compositing/visibility/visibility-simple-video-layer-expected.png
[modify]
https://crrev.com/540e2ecde447b0757dd5bb079a59d8faef3183c1/third_party/blink/web_tests/platform/win/compositing/visibility/visibility-simple-video-layer-expected.png

Comment 24 by michaelludwig@google.com on Fri, Mar 18, 2022, 9:11 AM EDT Project Member

Status: Fixed (was: Assigned)
Blockedon: -skia:10456

Comment 25 by xpsve...@gmail.com on Fri, Mar 18, 2022, 9:22 AM EDT

Hi,

Thank you for the fix. Is this security issue eligible for VRP bounty?

Thank you.

Comment 26 by sheriffbot on Fri, Mar 18, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 27 by sheriffbot on Fri, Mar 18, 2022, 1:41 PM EDT Project Member

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

Comment 28 by sheriffbot on Fri, Mar 18, 2022, 2:01 PM EDT Project Member

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

Requesting merge to extended stable M98 because latest trunk commit (982400) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (982400) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (982400) appears to be after beta branch point (972766).

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

Comment 29 by sheriffbot on Fri, Mar 18, 2022, 4:50 PM EDT 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 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 30 by sheriffbot on Fri, Mar 18, 2022, 4:50 PM EDT 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.
Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

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

Comment 31 by sheriffbot on Fri, Mar 18, 2022, 4:50 PM EDT 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 32 by michaelludwig@google.com on Mon, Mar 21, 2022, 9:55 AM EDT Project Member

Questions for m100, m99, and m98 since the answers are the same.

1. Security severity high (video content can escape and overlap with address bar, making it spoofable with the right video)
2. https://chromium-review.googlesource.com/c/chromium/src/+/3516507 (original CL)
3. First released in 101.0.4951.0
4. No
5. No
6. I don't think so, the bug was somewhat difficult to reproduce but the underlying cause is well understood and confirmed fixed in ToT. The fix should not interact with anything in m98, m99, or m100 to invalidate that.

Comment 33 by amyressler@chromium.org on Mon, Mar 21, 2022, 4:41 PM EDT Project Member

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

Hi Michael, thanks for the fix and responding to the bot's questionnaire; since is landing just prior to stable cut, I'm going to suggest we defer merging to stable 100 a bit later and getting this into first M100 stable respin

merge to M98 and M99 n/a, as there are no further planned releases of M98 extended or M99 stable

Comment 34 by amyressler@chromium.org on Mon, Mar 21, 2022, 4:44 PM EDT Project Member

In response to comment #25, thank you for the report. Any validated and fixed security bug in Chrome will be evaluated by the VRP Panel for a potential VRP reward. Your report should be reviewed by the VRP Panel at a panel session in the near future. Information about VRP reward will be updated directly on this bug. Thank you for your patience.

Comment 35 by amyressler@google.com on Wed, Mar 23, 2022, 3:46 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-3000

*** 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 36 by amyressler@chromium.org on Wed, Mar 23, 2022, 3:53 PM EDT Project Member

Congratulations - the VRP Panel has decided to award you $3,000 for this report. A member of our finance team will reach out to you soon to arrange payment. In the meantime, please let us know the name/handle/tag or other identifier you would like us to use in acknowledging you for this issue. Thank you again for your efforts and reporting this issue to us.

Comment 37 by xpsve...@gmail.com on Wed, Mar 23, 2022, 8:58 PM EDT

Wow, thank you for the reward and the timely fix! Please credit me under: Sven Dysthe

Comment 38 by amyressler@google.com on Fri, Mar 25, 2022, 4:58 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 39 by a_deleted_user on Mon, Mar 28, 2022, 5:26 PM EDT

Cc: -a_deleted_user

Comment 40 by amyressler@chromium.org on Thu, Mar 31, 2022, 2:53 PM EDT Project Member

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

M100 merge approved, please merge to branch 4896 at your earliest convenience so this fix can be included in the next M100 respin

Comment 41 by michaelludwig@google.com on Fri, Apr 1, 2022, 2:55 PM EDT Project Member

The merge is https://chromium-review.googlesource.com/c/chromium/src/+/3564640 but it is consistently failing on a win_optional_gpu_tests_rel try job. However, the specific tests shouldn't be effected by my CL, since it has nothing to do with webgl or typical compositing behavior in skia-renderer. I'm going to reach out to webgl test owner and see if this is expected when merging to a prior branch (in which case I'll just submit it), or figure out how to get the test to pass.

Comment 42 by michaelludwig@google.com on Fri, Apr 1, 2022, 4:39 PM EDT Project Member

I tested a white-space only change to skia_renderer.cc on branch 4896 and it also caused the win_optional_gpu_tests_rel job to fail, so I think that bot is just broken on m100. I will just skip that try job then.

Comment 43 by Git Watcher on Fri, Apr 1, 2022, 9:06 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/+/d88e959e018c8ec8107448c46879bd5537dfc0d1

commit d88e959e018c8ec8107448c46879bd5537dfc0d1
Author: Michael Ludwig <michaelludwig@google.com>
Date: Sat Apr 02 01:05:15 2022

[skia_renderer]: Use RectF::Intersect in ApplyScissor

(cherry picked from commit 540e2ecde447b0757dd5bb079a59d8faef3183c1)

~~Bug: 1299287~~, ~~1307317~~
Change-Id: I026090466ebfb3dee0e9daf0609f04babcf42092
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3516507
Reviewed-by: Kyle Charbonneau <kylechar@chromium.org>
Reviewed-by: Brian Sheedy <bsheedy@chromium.org>
Commit-Queue: Michael Ludwig <michaelludwig@google.com>
Cr-Original-Commit-Position: refs/heads/main@{#982400}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3564640
Cr-Commit-Position: refs/branch-heads/4896@{#1017}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[add]
https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/linux/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[add]
https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/linux/compositing/visibility/visibility-simple-video-layer-expected.png
[modify]
https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/win/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify]
https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/content/test/gpu/gpu_tests/test_expectations/pixel_exp

https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/content/test/gpu/gpu_tests/test_expectations/pixel_expectations.txt
[add] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/linux/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/win/images/yuv-decode-eligible/color-profile-layer-expected.png
[add] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/linux/virtual/threaded/compositing/visibility/visibility-simple-video-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/mac/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/mac/virtual/exotic-color-space/images/yuv-decode-eligible/color-profile-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/flag-specific/highdpi/compositing/geometry/video-fixed-scrolling-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/flag-specific/skia-vulkan-swiftshader/compositing/visibility/visibility-simple-video-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/mac/compositing/visibility/visibility-simple-video-layer-expected.png
[modify] https://crrev.com/d88e959e018c8ec8107448c46879bd5537dfc0d1/third_party/blink/web_tests/platform/win/compositing/visibility/visibility-simple-video-layer-expected.png

Comment 44 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT Project Member

Labels: Release-2-M100

Comment 45 by adetaylor@google.com on Mon, Apr 11, 2022, 1:29 PM EDT Project Member

Labels: CVE-2022-1306 CVE_description-missing

Comment 46 by sheriffbot on Fri, Jun 24, 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 47 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 48 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing