Starred by 4 users

Owner:	michaelludwig@google.com
CC:	michaelludwig@google.com kylec...@chromium.org bsalo...@google.com backer@chromium.org weiliangc@chromium.org
Status:	Fixed *(Closed)*
Components:	Internals>Compositing Internals>Skia>Compositing
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Severity-Medium
allpublic
reward-inprocess
Hotlist-Recharge-BouncingOwner
CVE_description-submitted
Target-97
M-97
external_security_report
FoundIn-96
Security_Impact-Extended
merge-merged-4692
merge-merged-97
Release-0-M97
CVE-2022-0116

Issue 1272250: Security: CSS transform and backface-visibility: hidden allow to render over Chrome UI

Reported by susah...@gmail.com on Sat, Nov 20, 2021, 5:36 PM EST

Code

After set large CSS transform scale, perspective CSS property, and backface-visibility to hidden interestingly the background-color or background-image will render over Chrome user interface including address bar and download bar.

As image able to render over Chrome UI I assume it's possible to perform address bar spoofing and other spoofing.

VERSION
Tested on following:
- Chrome 96.0.4664.45 (Official Build) (64-bit) on Windows 11
- Chrome Beta 97.0.4692.20 (Official Build) (64-bit) on Windows 11
- Chrome Dev Version 98.0.4710.4 (Official Build) (64-bit) on Arch Linux KDE X11
- Chrome Dev 98.0.4710.4 (Official Build) (64-bit) on Windows 11

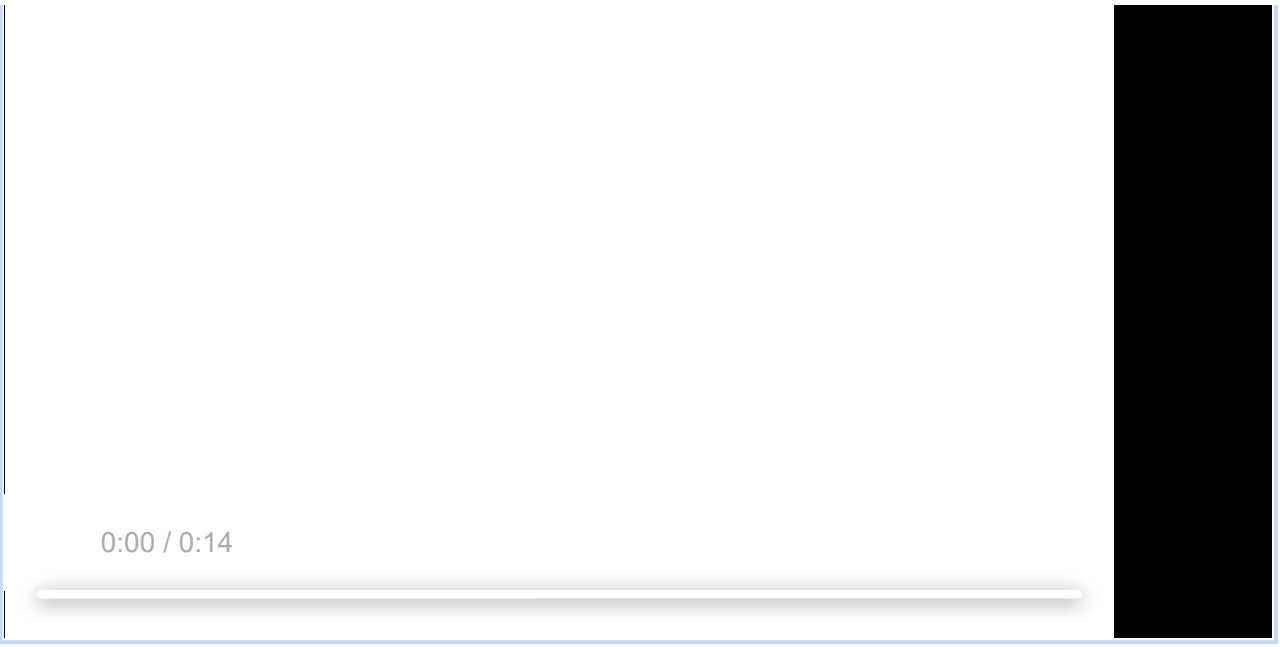
REPRODUCTION CASE
1. Visit attached renderover-backgroundimage.html
2. Chrome UI now covered by CSS background-image

(If it doesn't work on your device, try scrolling or zooming-in the page)

CREDIT INFORMATION
Reporter credit: Irvan Kurniawan (sourc7)

renderover-backgroundimage.html
476 bytes View Download

renderover-backgroundimage demonstration on Windows 11.mp4
238 KB View Download



Comment 1 by sheriffbot on Sat, Nov 20, 2021, 5:40 PM EST Project Member

Labels: external_security_report

Comment 2 by susah...@gmail.com on Sat, Nov 20, 2021, 5:45 PM EST

Reproduced on following Graphics Feature Status:
- Canvas: Hardware accelerated
- Canvas out-of-process rasterization: Disabled
- Compositing: Hardware accelerated
- Multiple Raster Threads: Enabled
- Out-of-process Rasterization: Hardware accelerated
- OpenGL: Enabled
- Rasterization: Hardware accelerated
- Raw Draw: Disabled
- Skia Renderer: Enabled
- Video Decode: Hardware accelerated
- Vulkan: Disabled
- WebGL: Hardware accelerated
- WebGL2: Hardware accelerated

Comment 3 by susah...@gmail.com on Sat, Nov 20, 2021, 5:56 PM EST

Look like it related to Skia Renderer, because when I toggle "Skia API for compositing" to "Disabled" I unable to reproduce the issue.

Comment 4 by mpdenton@chromium.org on Mon, Nov 22, 2021, 8:27 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: bsalomon@chromium.org

Cc: bsalo...@google.com michaelludwig@google.com kylec...@chromium.org
Labels: Security_Severity-Medium FoundIn-96 OS-Linux OS-Windows Pri-2
Components: Internals>Compositing Internals>Skia>Compositing

I don't see it draw over the UI (Linux Chrome 96.0.4664.45) but I do see my desktop background appearing in the viewport. Assigning to bsalomon@, could you please help me triage this one? (also adding people from previous similar bugs)

Comment 5 by sheriffbot on Mon, Nov 22, 2021, 8:27 PM EST Project Member

Labels: Security_Impact-Extended

Comment 6 by sheriffbot on Tue, Nov 23, 2021, 12:24 PM EST Project Member

Status: Untriaged (was: Assigned)
Owner: ----
Labels: Hotlist-Recharge-BouncingOwner

The assigned owner "bsalomon@chromium.org" is not able to receive e-mails, please re-triage.

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

Comment 7 by bsalo...@google.com on Tue, Nov 23, 2021, 12:26 PM EST Project Member

Status: Assigned (was: Untriaged)
Owner: bsalo...@google.com

Comment 8 by bsalo...@google.com on Tue, Nov 23, 2021, 12:43 PM EST Project Member

Making SkiaRenderer::CanExplictily scissor always return false works around this issue.

Comment 9 by sheriffbot on Tue, Nov 23, 2021, 12:52 PM EST Project Member

Labels: Target-97 M-97

Setting milestone and target because of medium severity.

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

Comment 10 by bsalo...@google.com on Tue, Nov 23, 2021, 1:08 PM EST Project Member

Status: Started (was: Assigned)
Owner: michaelludwig@google.com

Michael, going to turn this one over to you. The problem is that ApplyExplicitScissor() transforms the scissor rect to the quad space and the float coordinates are too large to accurately do the insetting. When the quad gets projected it draws well outside of the intended scissor. Here is an example device_transform from when the bug occurs:

|0 8.39062 0 -9.01124e+09|
|0 0 1 0|
|0 0 0 1|

Seems like we should refactor this so that if the reverse transform produces large (in abs terms) coords then we fall back to using a clip.

Comment 11 by bsalo...@google.com on Tue, Nov 23, 2021, 1:09 PM EST Project Member

Also, I was able to reproduce this with content_shell on linux by opening the html from the original post and scrolling down.

Comment 12 by sheriffbot on Tue, Nov 23, 2021, 1:18 PM EST Project Member

Labels: -Pri-2 Pri-1

Setting Pri-1 to match security severity Medium. 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 Git Watcher on Tue, Nov 30, 2021, 1:31 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/ab1b76f3e7cdad702c562f0b43bf3367caff4812

commit ab1b76f3e7cdad702c562f0b43bf3367caff4812
Author: Michael Ludwig <michaelludwig@google.com>
Date: Tue Nov 30 18:30:10 2021

[skia_renderer] - Don't explicitly clip scissor for large transforms

This adds a check to CanExplicitlyScissor that confirms that the device space scissor rect, transformed to the quad's local space, can be transformed back to device space and equal the same pixel bounds.

Without this check, sufficiently large scales and translates could cause the local-space coordinates of the scissor rect to be in a float range that does not have single-pixel precision, meaning it could round significantly. Clipping the quad's coordinates to those rounded edges and then transforming to device space can result in coordinates that fall outside the original device-space scissor rect.

If however, we ensure we can round-trip the scissor coordinates, then any clipping to the quad's coordinates will also be projected to within the scissor rect as well.

~~Bug: 1272250~~
Change-Id: I7c37c54efd082723797ccf32b5d19ef285c520c1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3306893
Commit-Queue: Michael Ludwig <michaelludwig@google.com>
Reviewed-by: Brian Salomon <bsalomon@google.com>
Reviewed-by: Kyle Charbonneau <kylechar@chromium.org>
Cr-Commit-Position: refs/heads/main@{#946552}

[modify] https://crrev.com/ab1b76f3e7cdad702c562f0b43bf3367caff4812/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/ab1b76f3e7cdad702c562f0b43bf3367caff4812/components/viz/service/display/skia_renderer.h

Comment 14 by michaelludwig@google.com on Tue, Nov 30, 2021, 3:09 PM EST Project Member

Status: Fixed (was: Started)

Comment 15 by sheriffbot on Wed, Dec 1, 2021, 12:42 PM EST Project Member

Labels: reward-topanel

Comment 16 by sheriffbot on Wed, Dec 1, 2021, 1:40 PM EST Project Member

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

Comment 17 by sheriffbot on Wed, Dec 1, 2021, 2:06 PM EST Project Member

Labels: Merge-Request-97

Requesting merge to beta M97 because latest trunk commit (946552) appears to be after beta branch point (938553).

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

Comment 18 by sheriffbot on Wed, Dec 1, 2021, 2:12 PM EST Project Member

Labels: -Merge-Request-97 Hotlist-Merge-Review Merge-Review-97

Merge review required: M97 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: benmason (Android), harrysouders (iOS), ceb (ChromeOS), pbommana (Desktop)

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

Comment 19 by michaelludwig@google.com on Wed, Dec 1, 2021, 3:49 PM EST Project Member

1. Yes, medium severity security bug fix that affects UI visuals, corrupted by page content.
2. https://chromium-review.googlesource.com/c/chromium/src/+/3306893 (original)
3. Yes, in 98.0.4740.0
4. No
5. N/A
6. N/A

Comment 20 by amyressler@chromium.org on Mon, Dec 6, 2021, 5:28 PM EST Project Member

Labels: -Merge-Review-97 Merge-Approved-97

merge approved for M97, please merge to branch 4692 ASAP /by 12pm PST tomorrow so this can be included in tomorrow's beta cut

Comment 21 by pbommana@google.com on Tue, Dec 7, 2021, 12:07 PM EST Project Member

Your change has been approved for M97 branch 4692,please go ahead and merge the CL's to M97 branch manually asap so that they would be part of tomorrows Beta release.thank you

Comment 22 by Git Watcher on Tue, Dec 7, 2021, 3:50 PM EST Project Member

Labels: -merge-approved-97 merge-merged-4692 merge-merged-97

The following revision refers to this bug:

https://chromium.googlesource.com/chromium/src/+/4deb522c22e748f223feae060203d50bfd740eb1

commit 4deb522c22e748f223feae060203d50bfd740eb1
Author: Michael Ludwig <michaelludwig@google.com>
Date: Tue Dec 07 20:49:07 2021

[skia_renderer] - Don't explicitly clip scissor for large transforms

This adds a check to CanExplicitlyScissor that confirms that the device space scissor rect, transformed to the quad's local space, can be transformed back to device space and equal the same pixel bounds.

Without this check, sufficiently large scales and translates could cause the local-space coordinates of the scissor rect to be in a float range that does not have single-pixel precision, meaning it could round significantly. Clipping the quad's coordinates to those rounded edges and then transforming to device space can result in coordinates that fall outside the original device-space scissor rect.

If however, we ensure we can round-trip the scissor coordinates, then any clipping to the quad's coordinates will also be projected to within the scissor rect as well.

(cherry picked from commit ab1b76f3e7cdad702c562f0b43bf3367caff4812)

~~Bug: 1272250~~
Change-Id: I7c37c54efd082723797ccf32b5d19ef285c520c1
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3306893
Commit-Queue: Michael Ludwig <michaelludwig@google.com>
Reviewed-by: Brian Salomon <bsalomon@google.com>
Reviewed-by: Kyle Charbonneau <kylechar@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#946552}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3320870
Auto-Submit: Michael Ludwig <michaelludwig@google.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/branch-heads/4692@{#786}
Cr-Branched-From: 038cd96142d384c0d2238973f1cb277725a62eba-refs/heads/main@{#938553}

[modify] https://crrev.com/4deb522c22e748f223feae060203d50bfd740eb1/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/4deb522c22e748f223feae060203d50bfd740eb1/components/viz/service/display/skia_renderer.h

Comment 23 by amyressler@chromium.org on Tue, Jan 4, 2022, 11:59 AM EST Project Member

Labels: Release-0-M97

Comment 24 by amyressler@google.com on Tue, Jan 4, 2022, 1:35 PM EST Project Member

Labels: CVE-2022-0116 CVE_description-missing

Comment 25 by amyressler@google.com on Thu, Jan 27, 2022, 8:03 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-1000

*** 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 26 by amyressler@chromium.org on Thu, Jan 27, 2022, 8:36 PM EST Project Member

Congratulations on another one! The VRP Panel has decided to award you $1,000 for this report. Thanks for your efforts and reporting this issue to us.

Comment 27 by amyressler@google.com on Fri, Jan 28, 2022, 8:13 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 28 by sheriffbot on Wed, Mar 9, 2022, 1:31 PM EST 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 29 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted