Starred by 2 users

Owner:	backer@chromium.org **Last visit > 30 days ago**
CC:	backer@chromium.org adetaylor@chromium.org ericrk@chromium.org wfh@chromium.org schenney@chromium.org khush...@chromium.org zmo@chromium.org achuith@chromium.org michaelludwig@google.com weiliangc@chromium.org bsalo...@google.com
Status:	Fixed *(Closed)*
Components:	Internals>Skia>Compositing
Modified:	May 1, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2020-01-02
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Needs-Feedback
reward-3000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
Target-79
M-79
merge-merged-3987
merge-merged-80
Release-0-M80
CVE-2020-6396

Issue 1035271: Security: 3D CSS transform and drop-shadow can draw over address bar

Reported by luc.r...@gmail.com on Wed, Dec 18, 2019, 12:01 AM EST

Code

VULNERABILITY DETAILS
When a block element has a 3D CSS transform (e.g. transform: translate3d), CSS filters such as drop-shadow and blur can draw outside of the webpage frame, including on top of the address bar. drop-shadow in particular can be used with a canvas element to draw arbitrarily chosen pixels in a given color. By combining several such elements with each target color, arbitrary images can be drawn over the address bar, reliably spoofing URLs.

This vulnerability only applies to certain environments; I'm not yet sure what causes a particular machine/environment to be vulnerable.

VERSION
Chrome Version: 79.0.3945.88 stable
Operating System: Arch Linux, updated 2019-12-17, with xmonad

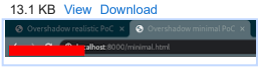
I've tested this on four machines meeting the above version description. Only two are affected, and I can't think of any obvious distinction separating them. I've also tested this on one Windows machine, which was not affected. If there's anything I can do to gather additional information about the machines involved, please let me know.

REPRODUCTION CASE
See attached minimal.html which, on affected browsers, draws a red box over the address bar. The attached screenshot.png shows what this looks like on my machine.

CREDIT INFORMATION
Reporter credit: William Luc Ritchie

minimal.html
312 bytes View Download

screenshot.png
13.1 KB View Download



Comment 1 by wfh@chromium.org on Wed, Dec 18, 2019, 1:25 PM EST Project Member

Status: Available (was: Unconfirmed)
Cc: wfh@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>Paint Blink>CSS

Thanks for the report. I'll try and repro and see if I can narrow down whether this is OS/distro specific and/or a recent regression...

Comment 2 by wfh@chromium.org on Wed, Dec 18, 2019, 3:28 PM EST Project Member

I can't reproduce this on any platforms I have access to. Perhaps this is specific to your window manager? Perhaps this is specific to your machine, can you paste your chrome://version list of variations?

Comment 3 by schenney@chromium.org on Thu, Dec 19, 2019, 7:39 AM EST Project Member

Labels: Needs-Feedback
NextAction: 2020-01-02

Comment 4 by sheriffbot@chromium.org on Thu, Dec 19, 2019, 9:43 AM EST Project Member

Labels: Target-79 M-79

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 monor...@bugs.chromium.org on Thu, Jan 2, 2020, 7:00 AM EST

The NextAction date has arrived: 2020-01-02

Comment 6 by adetaylor@google.com on Thu, Jan 9, 2020, 12:52 PM EST Project Member

Cc: schenney@chromium.org

wfh@, please would you make sure something appropriate happens to this bug in the absence of additional feedback? I suspect closing as WontFix is appropriate but as you've looked at it already, I wanted to leave it to you. Thanks.

Comment 7 by luc.r...@gmail.com on Fri, Jan 10, 2020, 2:58 AM EST

Sorry for lack of reply until now; I've been working on getting a reproducible case in a Vagrant VM. With further testing, I've discovered a few more details about what configurations are affected. I can now reproduce this on every Arch Linux machine that I've tested on. However:

1. Google Chrome is affected, but Chromium is not.
2. Google Chrome is not affected on first run, but after having been opened and closed once, it is affected on all subsequent runs. Without knowing the details of what's initialized after first run I can't really speculate very well, but one theory is that it may be related to variations, since on first run chrome://version does not list any.

I can reproduce this in multiple window managers, including XMonad (X11), Gnome (both X11 and Wayland), and Cinnamon (X11).

Earlier today I managed to reproduce the bug in a Vagrant VM, but only if 3D acceleration is enabled on the backing Virtualbox provider. I'm attaching a Vagrantfile that can demo this bug in one command. Frustratingly, it appears that some *host* machines don't display the bug behaviour in the Vagrant guest (!), which I think might come down to Virtualbox not actually enabling 3D acceleration on these machines.

I'm also attaching chrome://version dumps from each of the machines I've tested, including some unaffected configurations (Chromium, Google Chrome firstrun) for comparison.

machine3_affected_chrome_version.txt
2.3 KB View Download

machine2_unaffected_chromium_version.txt
557 bytes View Download

machine2_affected_chrome_version.txt
1.9 KB View Download

machine1_unaffected_chromium_version.txt
689 bytes View Download

machine1_unaffected_chrome_firstrun_version.txt
592 bytes View Download

machine1_affected_chrome_version.txt
1.9 KB View Download

machine4_affected_chrome_version.txt
2.2 KB View Download

Vagrantfile
3.1 KB View Download

Comment 8 by schenney@chromium.org on Fri, Jan 10, 2020, 9:54 AM EST Project Member

Components: -Blink>Paint -Blink>CSS Internals>GPU

Comment #7 points to hardware rendering being key to reproduction, so this looks like a viz compositor issue of some kind.

Comment 9 by schenney@chromium.org on Fri, Jan 10, 2020, 9:54 AM EST Project Member

Status: Untriaged (was: Available)

Comment 10 by mbarb...@chromium.org on Mon, Jan 13, 2020, 7:15 PM EST Project Member

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

danakj: Could you please take a look at this or help us find another owner?

Comment 11 by sheriffbot@chromium.org on Tue, Jan 14, 2020, 9:10 AM EST Project Member

danakj: Uh oh! This issue still open and hasn't been updated in the last 27 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 12 by danakj@chromium.org on Tue, Jan 14, 2020, 10:05 AM EST Project Member

Owner: khush...@chromium.org

Comment 13 by khush...@chromium.org on Tue, Jan 14, 2020, 1:28 PM EST Project Member

I can repro on M79 stable but not on M80 beta or M81 dev on a linux machine. I'm trying to verify if this is already fixed since in terms of GPU feature status there is no difference in my stable and dev builds.

luc.ritchie@, can you check if you can repro this on any canary/dev/beta?

Comment 14 by khush...@chromium.org on Tue, Jan 14, 2020, 2:05 PM EST Project Member

Cc: ericrk@chromium.org

Definitely looks like hardware acceleration (compositing) is needed to repro this but that's enabled by default on supported configurations on linux and we have no ongoing experiment to enable it via finch. And having it enabled on both stable and beta, the bug only reproes for me on beta.

This is what my finch config looks like:
AllowSyncXHRInPageDismissal-EnabledLaunch
AsyncStackAdTagging-Default
AutofillCompany-Default
AutofillNoLocalSaveOnUnmaskOrUploadSuccess-FullyEnabled_WithStartsActive
AutofillOverrideWithRaterConsensus-Preperiod_Enabled2_10
AutofillServerBehaviors-Default
BlinkSchedulerVeryHighPriorityForCompositingExperiments-Default
BlobDataPipeTuning-Enabled_2MB
CSSBackdropFilter-EnabledLaunch
CacheStorageEagerReading-Enabled3
CacheStorageHighPriorityMatch-Enabled5
CanvasAlwaysDeferral-Default
CertDualVerificationTrial-Default
CertVerifierBuiltin-Default
ChromeChannelStable-Enabled
ClickToCallV2Sender-Default_20191026
ClientSideDetectionModel-Model0
CloudPolicyOverFCM-Default
DefaultPassthroughCommandDecoder-Default
DialMediaRouteProvider-EnabledLaunch
DynamicTcmallocCacheSizes-Default
EnableSafetyTipUI-Default_20191122
EnterpriseReportingInBrowser-Default
ExpiredHistograms-ExpiredHistogramLogicEnabled
GlobalMediaControlsInProductHelp-Enabled
HeapProfiling-Default
HtmlImportsRequestInitiatorLockKillSwitch-Disabled_EmergencyKillSwitch
ImageDescriptions-EnabledLaunch
ImprovedCookieControlsStudy-Preperiod_Default
IndexedDBHighPriority-Default
KeepaliveRequestPriority-Default
LazyLoad-Default
LegacyTLSDeprecation-Default
LookalikeUrlNavigationSuggestionsUIV2-EnabledLaunch
MirroringService-EnabledLaunch
MixedAutoupgrade-Preperiod_Default
MixedContentShieldRemoval-EnabledLaunch
MojoChannelUnreadMessageQuota-Default
MostLikelyDesktopDeprecation-Default
MyChromeEverywhere-Default
NTPRicherPickerAndColors-EnableRicherPickerWithColors
NativeNotifications-Disabled_Dogfood
OffMainThreadServiceWorkerStartup-Default
OmniboxBundledExperimentV1-Stable_Desktop_OmniboxFakeboxDemotion_Launch_V2_Enabled_Postperiod
OmniboxDocumentProviderDogfood-Stable_Desktop_OmniboxDocumentProvider_Experiment_Dogfood_V2
OmniboxMaterialDesignWeatherIcons-All_OmniboxMaterialDesignWeatherIcons_Enabled
OmniboxMaxMatchesURLLimitLaunch-Desktop_OmniboxMaxMatchesWithURLLimit_Enabled_V2
OutOfBlinkCors-Default
PaintHolding-Default
PasswordLeakDetection-Enabled_Dogfood
PauseBrowserInitiatedHeavyTrafficForP2P-Enabled_Dogfood
ProfileMenuRevampIdentityPill-EnabledLaunch
ProtoDBSharedMigration-Default
QUIC-EnabledNoId
SafeBrowsingAdPopupTrigger-Default
SafeBrowsingAdRedirectTrigger-Default
SafeBrowsingRealTimeUrlLookupEnabled-Default
SafeBrowsingRealTimeUrlLookupFetchAllowlist-EnabledLaunch
ServiceWorkerStartupOptimizations-Default
SharedClipboard-Default
SimpleCacheTrailerPrefetchHint-Default
SqlSkipPreload-Default
StaticHostQuota-Control20191011
SyncButterWallet-EnabledLaunch
TabHoverCards-EnabledLaunch
TranslateRankerModel-launch_20180628_model_20170329_with_blacklist_override_default_v2
TrustedTypes-Enabled_Dogfood
UKM-Enabled_20180314
UMA-Population-Restrict-dogfood
UMA-Uniformity-Trial-1-Percent-group_55
UMA-Uniformity-Trial-10-Percent-default
UMA-Uniformity-Trial-100-Percent-group_01
UMA-Uniformity-Trial-20-Percent-group_02
UMA-Uniformity-Trial-5-Percent-group_13
UMA-Uniformity-Trial-50-Percent-default
UkmSamplingRate-Sampled
UmaAndUkmDemographics-UMA_Control
UnidoOnSignIn-Preperiod_Default
UseSkiaRenderer-EnabledLaunch
UseTextForUpdateButton-Default
V8BytecodeFlushing-Default
V8WasmCodeCache-EnabledLaunch
VerifyHTMLFetchedFromAppCacheBeforeDelay-Default
VizHitTest-VizHitTestSurfaceLayer

SkiaRenderer is now enabled by default so can't be that if its a finch variation causing it and nothing else looks suspicious to me. +ericrk on this too.
luc.ritchie@, it would be good to see your chrome://gpu status page as well. My inkling right now is that the bug may already be fixed. And if the fix is on beta then there is nothing actionable here to do.

Comment 15 by luc.r...@gmail.com on Tue, Jan 14, 2020, 2:20 PM EST

I can still repro this on both 80.0.3987.42 and 81.0.4021.2 (AUR packages google-chrome-beta and google-chrome-dev). On both of those versions, first run is also affected. Comparing chrome://gpu seems to confirm that I can repro if and only if SkiaRenderer is enabled - it's always enabled for me on M80 and above, but on M79 it's only enabled for me after first run.

GPU and version dumps attached.

machine1_unaffected_chrome_firstrun_gpu.txt
12.9 KB View Download

machine1_dev_affected_chrome_version.txt
634 bytes View Download

machine1_dev_affected_chrome_gpu.txt
12.4 KB View Download

machine1_beta_affected_chrome_subsequent_version.txt
2.3 KB View Download

machine1_beta_affected_chrome_gpu.txt
12.4 KB View Download

machine1_beta_affected_chrome_firstrun_version.txt
604 bytes View Download

machine1_affected_chrome_subsequent_gpu.txt
12.4 KB View Download

Comment 16 by khush...@chromium.org on Tue, Jan 14, 2020, 2:25 PM EST Project Member

Cc: backer@chromium.org

Interesting. Could you go to chrome://flags/#enable-skia-renderer and mark this flag as disabled. You should see SkiaRenderer disabled on the chrome://gpu page after this. And check if it still reproes?

On my linux machine I'm unable to repro this with SkiaRenderer enabled. Could possibly be a GPU driver bug in that case.

Comment 17 by khush...@chromium.org on Tue, Jan 14, 2020, 2:26 PM EST Project Member

Cc: zmo@chromium.org

Comment 18 by khush...@chromium.org on Tue, Jan 14, 2020, 2:29 PM EST Project Member

Owner: backer@chromium.org

Sorry my bad. The fact that it reproes on M79 stable on my device means its not a driver bug. And I can't repro it with SkiaRenderer disabled on my stable build either. So it is indeed SkiaRenderer.

Comment 19 by ericrk@chromium.org on Tue, Jan 14, 2020, 2:32 PM EST Project Member

Cc: khush...@chromium.org

Comment 20 by khush...@chromium.org on Tue, Jan 14, 2020, 2:35 PM EST Project Member

Components: -Internals>GPU Internals>Skia>Compositing

I'm still confused about why it won't repro on dev/beta and a local build for me when it did on stable. But given the fact that its fixed means a bisect locally is a good idea to identify what fixed it and whether the fix ended up being GPU specific.

Comment 21 by michaelludwig@google.com on Tue, Jan 14, 2020, 3:22 PM EST Project Member

If it helps with the bisecting, the RPDQ bypass work on SkiaRenderer just missed m79 and then landed in m80. It perhaps fixed a bug in calculating the render pass bounds w/o realizing it. The visual effect looks similar to what I'd expect if the code thought it could drop the scissor rect for the viewport because the draw quad was completely contained in it, but after the filtering would have affected it.

Also somewhat related, but maybe not exactly, is this CL: https://skia-review.googlesource.com/c/skia/+/259137, which made it into m81. This applied to the drop shadow sigma, though, whereas this minimal test case manipulates offset.

Have we added unit tests for this scenario?

Comment 22 by luc.r...@gmail.com on Tue, Jan 14, 2020, 9:43 PM EST

For me, turning off #enable-skia-renderer stops the bug from occurring, turning it on means I still get the bug even on beta and dev. Based on chrome://gpu it looks like the default value of the flag was different between Chromium, Chrome first run, and Chrome later runs, and also stable vs beta vs dev. On any of them, if I force it, Skia on => bug, Skia off => no bug.

One point when bisecting: if the "Chrome isn't your default browser" bar shows up, it appears to render in front of the shadow, so it's probably a good idea to click through or use a test page with a tall enough drop shadow to reach past the bar.

Comment 23 by backer@chromium.org on Thu, Jan 23, 2020, 4:31 PM EST Project Member

I can reproduce in my stable M79 browser, but I cannot repro in M80 official build (80.0.3987.9):

I bisected the fix for Chromium to this range:

https://chromium.googlesource.com/chromium/src/+log/5f66421b98cb2c673ec052e095773ca8d3a02b84..a7ae309060d5106243ed4353fb2828d35729d93d

I'm guessing it's this that fixed it:
https://chromium.googlesource.com/chromium/src/+/a7ae309060d5106243ed4353fb2828d35729d93d

Chromium dash says that is coming out in M80 (first release 80.0.3955.4):
https://chromiumdash.appspot.com/commits?commit=a7ae309060d5106243ed4353fb2828d35729d93d&platform=Linux

I'm trying to bisect official builds to see if anything different happens...

Comment 24 by backer@chromium.org on Thu, Jan 23, 2020, 4:56 PM EST Project Member

Official build bisect gives me https://chromium.googlesource.com/chromium/src/+log/80.0.3949.0..80.0.3950.0?pretty=full

This also contains Michael's change: https://chromiumdash.appspot.com/commit/a7ae309060d5106243ed4353fb2828d35729d93d

I'm guessing 3950 was never release publically, which is why it predates 3955.4

I will try merging this CL onto M79 to see if it is even feasible...

Comment 25 by backer@chromium.org on Thu, Jan 23, 2020, 5:25 PM EST Project Member

Labels: Merge-Request-79

This is not a trivial merge. It is based upon some CLs that were not merged to branch.

Merge CL is here: https://chromium-review.googlesource.com/c/chromium/src/+/2018185

It passes cc_unittests, viz_unittests and fixes the build of chrome.

@michaelludwig: Can you comment about the risk of the merge?

I'm pretty comfortable because the tests pass and this code has been on beta for quite some time.

Adding merge request.

Comment 26 by michaelludwig@google.com on Fri, Jan 24, 2020, 12:33 PM EST Project Member

I spent a little more time today looking at why it was failing, and why those bisected changes fixed it. There are two ways an image filter is applied in skia_renderer: on the paint of a draw, and as part of a save layer. When using a save layer, we add a clip to the filter bounds to limit the size of the saved layer. It turns out that the filter bounds already incorporated the quad's clip rect, so would prevent this type of overdraw, even though that was not the clip's intended purpose. Most RPDQs don't use a save layer, though, and store the filter on the paint so that Skia can manage the saved layer automatically if needed. In that case, the filter bounds were never added (since for the original layer-size restricting purpose, Skia could be just as efficient, if not more so, using the actual draw geometry and filter properties).

With the big RPDQ refactor, bypassed solid color quads would skip allocating a render pass, but would have to use the saveLayer version because that draw call doesn't accept an SkPaint. This meant that the minimal reproduction test appeared to be fixed.

Unfortunately, after tracing out all this logic, I was able to modify the test case to reproduce on ToT still. As long as the div with the drop shadow has its content as a tile or another renderpass, it'll use the paint+imagefilter route. The scissor rect of the window is explicitly clipped to the quad's visible rect, pre-filtering, instead of post-filtering. I have a CL here that updates the explicit scissor logic to not apply it if it's a RPDQ with filters: https://chromium-review.googlesource.com/c/chromium/src/+/2019804

The good news is it's a lot simpler and should be a more straight forward cherry-pick to 79 or earlier.

Comment 27 by sheriffbot@chromium.org on Fri, Jan 24, 2020, 1:05 PM EST Project Member

Status: Fixed (was: Assigned)

Please mark security bugs as fixed as soon as the fix lands, and before requesting merges. This update is based on the merge- labels applied to this issue. Please reopen if this update was incorrect.

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

Comment 28 by bugdroid on Fri, Jan 24, 2020, 1:44 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/9b174c64e9408d1b3f9c8b40514fa31e35b45227

commit 9b174c64e9408d1b3f9c8b40514fa31e35b45227
Author: Michael Ludwig <michaelludwig@google.com>
Date: Fri Jan 24 18:40:52 2020

Preserve scissor for RPDQs with filters

If the RPDQ has a filter, it's touched pixels are not actually restricted
to the visible rect of the quad. In that case it is incorrect to explicitly
clip the visible rect to the scissor and not set the scissor as a clipRect.
This CL makes it so the scissor is remembered and is applied post-filtering,
so effects like drop shadows are properly clipped to the window content.

~~Bug: 1035274~~
Change-Id: I138b1412c55489aa0068cc0ea1744a3248738716
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2019804
Reviewed-by: Jonathan Backer <backer@chromium.org>
Commit-Queue: Michael Ludwig <michaelludwig@google.com>
Cr-Commit-Position: refs/heads/master@{#735025}

[modify] https://crrev.com/9b174c64e9408d1b3f9c8b40514fa31e35b45227/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/9b174c64e9408d1b3f9c8b40514fa31e35b45227/components/viz/service/display/skia_renderer.h

Comment 29 by sheriffbot@chromium.org on Sat, Jan 25, 2020, 12:24 PM EST Project Member

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

Comment 30 by backer@chromium.org on Mon, Jan 27, 2020, 9:56 AM EST Project Member

Labels: Merge-Request-80

Adding merge request for M80 for #28 as well. Stable cut is tomorrow. It would like to get that in for our Linux users, where SkiaRenderer has been on by default since M78.

The CL is #28 is easy to merge and appears to be very low risk (thanks Michael!). I have confirmed that there are no related crash stack signatures on our Windows [1] and Android [2] SkiaRenderer Canary finch experiments. This is safe to merge. Unfortunately, I won't get UMA stats on crash rates for a few more days.

[1] https://crash.corp.google.com/browse?q=product_name%3D%27Chrome%27+AND+expanded_custom_data.ChromeCrashProto.channel%3D%27canary%27+AND+expanded_custom_data.ChromeCrashProto.ptype%3D%27gpu-process%27+AND+EXISTS%28SELECT+1+FROM+UNNEST%28expanded_custom_data.ChromeCrashProto.experiments.ids%29+expId+WHERE+expId%3D%226a2df91f-3f4a17df%22%29+AND+product.Version%3E%3D%2781.0.4038.2%27

[2] https://crash.corp.google.com/browse?q=product_name%3D%27Chrome_Android%27+AND+expanded_custom_data.ChromeCrashProto.channel%3D%27canary%27+AND+expanded_custom_data.ChromeCrashProto.ptype%3D%27gpu-process%27+AND+EXISTS%28SELECT+1+FROM+UNNEST%28expanded_custom_data.ChromeCrashProto.experiments.ids%29+expId+WHERE+expId%3D%226a2df91f-3f4a17df%22%29+AND+product.Version%3E%3D%2781.0.4038.2%27

Comment 31 by sheriffbot@chromium.org on Mon, Jan 27, 2020, 9:58 AM EST Project Member

Labels: -Merge-Request-80 Merge-Review-80 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://goto.google.com/chrome-release-branch-merge-guidelines
- 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: govind@(Android), Kariahda@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 32 by srinivassista@google.com on Mon, Jan 27, 2020, 12:00 PM EST Project Member

Labels: -Merge-Review-80 Merge-Approved-80

Approved for Merge to M80, branch:3987 pls merge your changes to the branch asap.

Comment 33 by natashapabrai@google.com on Mon, Jan 27, 2020, 1:42 PM EST Project Member

Labels: reward-topanel

Comment 34 by bugdroid on Mon, Jan 27, 2020, 3:45 PM EST Project Member

Labels: -merge-approved-80 merge-merged-3987 merge-merged-80

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/5cf10da1527d2cb4bc3bb7a1d3d143f44a1d8748

commit 5cf10da1527d2cb4bc3bb7a1d3d143f44a1d8748
Author: Michael Ludwig <michaelludwig@google.com>
Date: Mon Jan 27 20:44:51 2020

M80 merge: Preserve scissor for RPDQs with filters

Cherry pick of https://chromium-review.googlesource.com/c/chromium/src/+/2019804

If the RPDQ has a filter, it's touched pixels are not actually restricted
to the visible rect of the quad. In that case it is incorrect to explicitly
clip the visible rect to the scissor and not set the scissor as a clipRect.
This CL makes it so the scissor is remembered and is applied post-filtering,
so effects like drop shadows are properly clipped to the window content.

~~Bug: 1035271~~
Change-Id: I138b1412c55489aa0068cc0ea1744a3248738716
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2023350
Reviewed-by: Jonathan Backer <backer@chromium.org>
Commit-Queue: Jonathan Backer <backer@chromium.org>
Cr-Commit-Position: refs/branch-heads/3987@{#721}
Cr-Branched-From: c4e8da9871cc266be74481e212f3a5252972509d-refs/heads/master@{#722274}

[modify] https://crrev.com/5cf10da1527d2cb4bc3bb7a1d3d143f44a1d8748/components/viz/service/display/skia_renderer.cc
[modify] https://crrev.com/5cf10da1527d2cb4bc3bb7a1d3d143f44a1d8748/components/viz/service/display/skia_renderer.h

Comment 35 by backer@chromium.org on Mon, Jan 27, 2020, 4:12 PM EST Project Member

Should we merge to M79? I think this would merge cleanly. I don't feel like I am qualified to make that decision though.

Comment 36 by srinivassista@google.com on Tue, Jan 28, 2020, 10:58 AM EST Project Member

Cc: adetaylor@chromium.org

At this juncture M79 merge and a re-spin is not feasible with M80 right around the corner (next week),. we will wait for this fix to go out in M80.

Adding adetaylor@ in case he thinks otherwise.

Comment 37 by adetaylor@chromium.org on Tue, Jan 28, 2020, 11:58 AM EST Project Member

Labels: -Merge-Request-79

No need to merge this back to M79. Thanks though.

Comment 38 by natashapabrai@google.com on Wed, Jan 29, 2020, 7:01 PM EST 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 39 by natashapabrai@google.com on Wed, Jan 29, 2020, 7:12 PM EST Project Member

Congrats! The Panel decided to award $3,000 for this report!

Comment 40 by natashapabrai@google.com on Wed, Jan 29, 2020, 7:18 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 41 by adetaylor@google.com on Sat, Feb 1, 2020, 8:13 PM EST Project Member

Labels: Release-0-M80

Comment 42 by adetaylor@chromium.org on Mon, Feb 3, 2020, 6:47 PM EST Project Member

Labels: CVE-2020-6396 CVE_description-missing

Comment 43 by schenney@chromium.org on Wed, Feb 5, 2020, 5:41 PM EST Project Member

~~Issue 1048014~~ has been merged into this issue.

Comment 44 by adetaylor@chromium.org on Mon, Feb 10, 2020, 4:37 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 45 by adetaylor@google.com on Wed, Mar 4, 2020, 1:44 PM EST Project Member

Cc: achuith@chromium.org

Comment 46 by sheriffbot on Fri, May 1, 2020, 2:55 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