Starred by 2 users

Owner:	msw@chromium.org
CC:	sahir...@microsoft.com bsep@chromium.org csharrison@chromium.org hferr...@igalia.com msw@chromium.org caseq@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>Input
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

reward-2000
M-100
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
FoundIn-86
external_security_report
Target-94
Target-96
FoundIn-92
FoundIn-94
Security_Impact-Extended
Merge-NA-100
Release-0-M100
CVE-2022-1138

Issue 1246188: Security: Compromised renderer can set custom cursor up to 1024px over browser UI and other windows

Reported by alesa...@alesandroortiz.com on Thu, Sep 2, 2021, 7:32 PM EDT

Code

VULNERABILITY DETAILS

A compromised renderer can render large custom cursors over browser UI and other windows.

Mitigations for these issues were implemented in the renderer only, therefore a compromised renderer can bypass them:
~~Issue 1099276~~
~~Issue 880863~~
~~Issue 640227~~

Specifically, these mitigations can be bypassed:
* Limit custom cursor size to 128x128px:
https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/input/event_handler.cc;l=594;drc=289a8d63ffde8000d54fc338d9de25a0f12cd5c5

* Fallback to default cursor if custom cursor (32x32px or larger) renders outside page:
https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/input/event_handler.cc;l=619;drc=289a8d63ffde8000d54fc338d9de25a0f12cd5c5

The only notable browser-side enforcement is a 1024px custom cursor size enforcement:
https://source.chromium.org/chromium/chromium/src/+/main:content/common/cursors/webcursor.cc;l=25;drc=8bcc3b52806612784b034560bfff2c8bd8576a7a

Enforcing these mitigations in the browser side, especially the custom cursor size, would result in effective protections. This comment also points out the same thing:
https://source.chromium.org/chromium/chromium/src/+/main:third_party/blink/renderer/core/input/event_handler.cc;l=603;drc=289a8d63ffde8000d54fc338d9de25a0f12cd5c5
> // TODO(csharrison): Consider sending a fallback cursor in the IPC to the
> // browser process so we can do that calculation there instead, this would
> // ensure even a compromised renderer could not obscure browser UI with a
> // large cursor. [...]

The PoC provided is basic and only demonstrates a cursor rendering over browser UI. An improved PoC likely could overlay the omnibar and other security surfaces regardless of cursor position using the largest cursor possible (similar to https://jameshfisher.github.io/cursory-hack/ but with more flexibility on cursor position due to larger cursor size limit).

Screen recording note: The cursor rendering lag is more apparent in the recording than when viewed directly on screen. It's also a local build, so it may have more lag than production builds.

VERSION

Chrome Version:
Should repro on Stable: 92.0.4515.159 (Official Build) (64-bit) (cohort: Stable)
Verified repro on patched local build (~Aug 6th checkout): 94.0.4600.0 Revision e53e18d4b512d8ebaf1bcb591c3058af98d7ad18-refs/heads/master@{#909170}

Operating System: Windows 10 OS Version 2009 (Build 19042.1110)

Nothing of relevance has changed since my ~Aug 6th checkout, so should still repro on ToT

Nothing of relevance has changed since my ~Aug 6th checkout, so should still repro on Tot.

REPRODUCTION CASE
Setup:
1. Apply renderer.patch and rebuild Chromium to simulate compromised renderer with disabled mitigations.

Basic PoC:
Prerequsite: Compromised/patched renderer.
1. Navigate to https://alesandroortiz.com/security/chromium/cursor-large.html
2. Move cursor around page to observe behavior near window borders and near browser UI at top of window.

Observed: Large cursor is allowed to render over browser UI and outside browser window due to limited browser-side enforcement.
Expected: Large cursor is unable to render over browser UI or outside browser window because of browser-side enforcement.

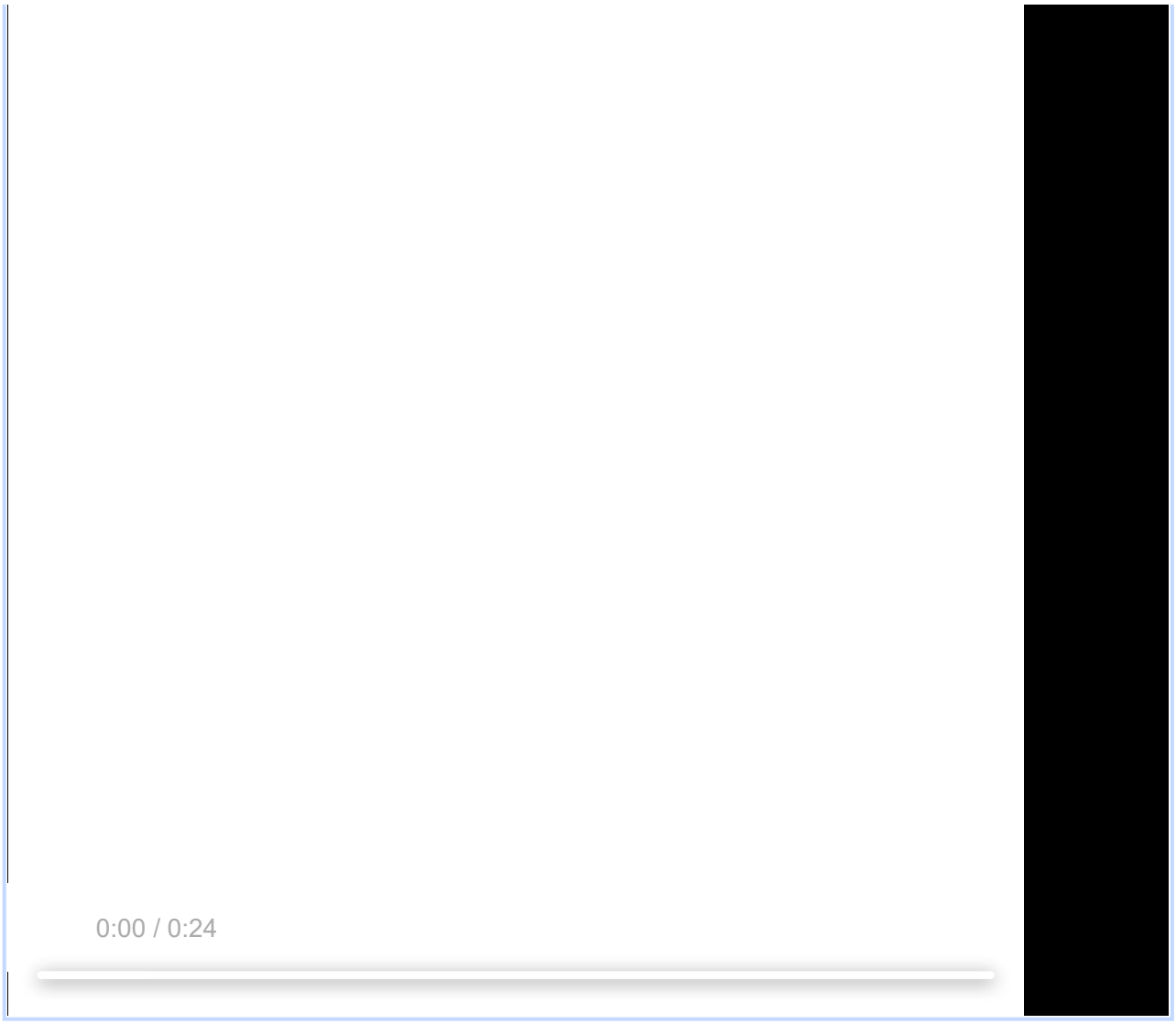
CREDIT INFORMATION
Reporter credit: Alesandro Ortiz <https://AlesandroOrtiz.com>

cursor-large.html
970 bytes View Download

cursor-images.zip
28.7 KB Download

renderer.patch
2.9 KB View Download

large-cursor.mp4
1.9 MB View Download



Comment 1 by alesa...@alesandroortiz.com on Thu, Sep 2, 2021, 7:36 PM EDT

Repro steps addendum:
3. Append ?cursor=1024 for the largest cursor size (see page for other available sizes).

Note that 1200px size is a demonstration that cursor size above 1024px is prevented by browser-side enforcement.

Comment 2 by sheriffbot on Thu, Sep 2, 2021, 7:37 PM EDT Project Member

Labels: external_security_report

Comment 3 by cthomp@chromium.org on Thu, Sep 2, 2021, 8:03 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: csharrison@chromium.org
Labels: Security_Severity-Medium FoundIn-86 FoundIn-92 FoundIn-94 OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: Blink>Input

Thanks for the detailed report (and for the video :D)! Setting this as Severity-Medium (as this can allow partial spoofing of trusted browser UI, but does not seem usable for complete control of the Omnibox that a Sev-High would entail), and FoundIn-86 (per blame on the linked code this dates to at least M-86, although that was the addition of more renderer side

FoundIn-86 (per blame on the linked code this dates to at least M-86, although that was the addition of more renderer-side checks so this likely goes back further).

Per the linked TODO, csharisson@ could you take this bug or find someone who could work on adding browser-side enforcement?

Comment 4 by sheriffbot on Thu, Sep 2, 2021, 8:07 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 5 by sheriffbot on Sat, Sep 4, 2021, 12:51 PM EDT Project Member

Labels: Target-94 M-94

Setting milestone and target because of medium severity.

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

Comment 6 by sheriffbot on Fri, Sep 17, 2021, 12:21 PM EDT Project Member

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

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

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

Thanks for your time! To disable nags, add the Disable-Nags label.

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

Comment 7 by alesa...@alesandroortiz.com on Tue, Sep 21, 2021, 8:08 PM EDT

cthomp@ or current sheriff: Current owner is OOO until Sep 27, up to you if you want to reassign or wait. I'm okay waiting since it requires a compromised renderer, so it's not a casual attack.

Comment 8 by sheriffbot on Fri, Oct 1, 2021, 12:21 PM EDT Project Member

csharrison: Uh oh! This issue still open and hasn't been updated in the last 28 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 9 by alesa...@alesandroortiz.com on Thu, Nov 11, 2021, 5:23 PM EST

Friendly ping: Any updates on this issue? No notable crbug activity since report creation in early September and don't see an open CL.

Comment 10 by sheriffbot on Mon, Nov 15, 2021, 12:22 PM EST Project Member

Labels: -M-94 Target-96 M-96

Comment 11 by csharrison@chromium.org on Thu, Nov 18, 2021, 1:21 PM EST Project Member

Cc: bsep@chromium.org msw@chromium.org

Hey sorry for the delay on this. FWIW this is not a regression. Cursor size attacks have always been possible in the renderer and our only protection was always the max size enforced on the browser.

I am probably not the right owner to implement the browser-side protections. But it seems pretty reasonable to make the browser-side enforcement match the blink max size of 128 px. +msw and bsep, do you see this change regressing any other features? Would one of you be willing to take ownership of this bug?

Comment 12 by alesa...@alesandroortiz.com on Fri, Jan 14, 2022, 6:08 PM EST

Friendly ping: Any updates on this issue? Last comment was looking for a new owner.

Comment 13 by csharrison@chromium.org on Thu, Jan 20, 2022, 10:53 AM EST Project Member

Status: Untriaged (was: Assigned)
Owner: ----
Cc: csharrison@chromium.org hferr...@igalia.com sahir...@microsoft.com

Moving myself to cc and adding a couple more folks that seem relevant.

Comment 14 by msw@google.com on Thu, Jan 20, 2022, 12:57 PM EST Project Member

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

Sorry for the lack of followup; I'm not aware of any valid use cases for such large custom cursor sizes offhand.
I couldn't find any original reasoning for Blink's 128px maximum in particular; it may have been added here:
https://src.chromium.org/viewvc/blink/trunk/Source/WebCore/page/EventHandler.cpp?annotate=136919&pathrev=136919
Still, making WebCursor's 1024px size from https://codereview.chromium.org/147193 match Blink's 128 from third_party/blink/renderer/core/input/event_handler.cc sgtm.
I'll see if I can write up a quick patch.

Comment 15 by msw@google.com on Fri, Jan 21, 2022, 8:32 PM EST Project Member

Hmm, even with that patch applied, I can't repro on ToT 100.0.4845.0 (Developer Build) (64-bit).
The cursor appears to be smaller than 128px, regardless of what query I use on the page.
I'll look closer next week.

Comment 16 by hferr...@igalia.com on Mon, Jan 24, 2022, 6:28 AM EST Project Member

Labels: -OS-Linux

msw: just in case, this bug doesn't affect Linux at the moment, since there's a bug in which the maximum cursor size is always 64px: https://crbug.com/1204322.

Comment 17 by msw@google.com on Mon, Jan 24, 2022, 6:38 PM EST Project Member

Thanks for that info! afaict, linux-chromeos also doesn't repro (likely for the same reason), but neither does Windows over Chrome Remote Desktop from Linux.
I'll try building on my local Windows or Mac devices soon.

I'll try building on my local Windows or Mac devices soon.

Comment 18 by hferr...@igalia.com on Mon, Jan 24, 2022, 7:22 PM EST Project Member

linux-chromeos should reproduce unless the hardware doesn't support those cursors, which is unlikely. I'm not sure if CRD imposes any limitations to the cursor though.

Comment 19 by msw@chromium.org on Tue, Jan 25, 2022, 2:14 PM EST Project Member

Status: Started (was: Assigned)

I was able to repro on a local Windows machine. I have a CL up for review at https://crrev.com/c/3413912

Comment 20 by Git Watcher on Thu, Jan 27, 2022, 8:50 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2

commit 868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2
Author: Mike Wasserman <msw@chromium.org>
Date: Fri Jan 28 01:49:41 2022

Make web cursor size limits match on browser and renderer

Use NSCursor arrowCursor on Mac for ui::mojom::CursorType::kNull.
(i.e. when WebCursor is constructed with an overly large custom cursor)

~~Bug: 1246188~~
Test: Automated unit tests and WPTs
Change-Id: I89627fa13cba96b755b8f80adbc91cfc865b6b1b
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3413912
Reviewed-by: Henrique Ferreiro <hferreiro@igalia.com>
Reviewed-by: Charlie Harrison <csharrison@chromium.org>
Commit-Queue: Mike Wasserman <msw@chromium.org>
Auto-Submit: Mike Wasserman <msw@chromium.org>
Cr-Commit-Position: refs/heads/main@{#964378}

[modify] https://crrev.com/868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2/content/common/cursors/webcursor_mac.mm
[modify] https://crrev.com/868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2/content/common/cursors/webcursor.cc
[modify] https://crrev.com/868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2/content/common/cursors/webcursor_unittest.cc

Comment 21 by msw@chromium.org on Fri, Jan 28, 2022, 12:57 PM EST Project Member

Status: Fixed (was: Started)
Labels: -M-96 M-100

Comment 22 by sheriffbot on Fri, Jan 28, 2022, 1:41 PM EST Project Member

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

Comment 23 by alesa...@alesandroortiz.com on Sun, Jan 30, 2022, 3:45 AM EST

Thanks for fixing, msw!

Comment 24 by sheriffbot on Sun, Jan 30, 2022, 12:41 PM EST Project Member

Labels: reward-topanel

Comment 25 by Git Watcher on Mon, Jan 31, 2022, 8:48 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/38a8343085e53889eba48fcff78a6c2295927333

commit 38a8343085e53889eba48fcff78a6c2295927333
Author: Mike Wasserman <msw@chromium.org>
Date: Tue Feb 01 01:47:47 2022

Revert "Make web cursor size limits match on browser and renderer"

This reverts commit 868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2.

Reason for revert: ~~https://crbug.com/1292426~~

Original change's description:
> Make web cursor size limits match on browser and renderer
>
> Use NSCursor arrowCursor on Mac for ui::mojom::CursorType::kNull.
> (i.e. when WebCursor is constructed with an overly large custom cursor)
>
> ~~Bug: 1246188~~
> Test: Automated unit tests and WPTs
> Change-Id: I89627fa13cba96b755b8f80adbc91cfc865b6b1b
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3413912
> Reviewed-by: Henrique Ferreiro <hferreiro@igalia.com>
> Reviewed-by: Charlie Harrison <csharrison@chromium.org>
> Commit-Queue: Mike Wasserman <msw@chromium.org>
> Auto-Submit: Mike Wasserman <msw@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#964378}

~~Bug: 1246188~~
Change-Id: Id7b3b88e65c012993537ce96c2b5064b7b76646e
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3428347
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Mike Wasserman <msw@chromium.org>
Cr-Commit-Position: refs/heads/main@{#965475}

[modify] https://crrev.com/38a8343085e53889eba48fcff78a6c2295927333/content/common/cursors/webcursor_mac.mm
[modify] https://crrev.com/38a8343085e53889eba48fcff78a6c2295927333/content/common/cursors/webcursor.cc
[modify] https://crrev.com/38a8343085e53889eba48fcff78a6c2295927333/content/common/cursors/webcursor_unittest.cc

Comment 26 by hferr...@igalia.com on Tue, Feb 1, 2022, 5:34 AM EST Project Member

Status: Assigned (was: Fixed)

msw: regarding ~~https://crbug.com/1292426~~, I think the problem is https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/devtools/devtools_eye_dropper.cc;l=196;drc=2759dc1223b322b24ff64d6c96ff3822e0e8851e, where the color picker cursor size is 150 pixels.

Comment 27 by msw@chromium.org on Tue, Feb 1, 2022, 12:54 PM EST Project Member

Status: Started (was: Assigned)
Cc: caseq@chromium.org

Thanks for the quick diagnosis there, hferreiro! +CC FYI caseq@chromium.org
Simply increasing WebCursor's limit 128->150px keeps DevToolsEyeDropper working.
That seems like an easy fix that still avoids significant abuse by compromised renders.
Please raise any objections to that approach here or on https://crrev.com/c/3428624

Comment 28 by Git Watcher on Tue, Feb 1, 2022, 4:17 PM EST Project Member

Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1665a1d16d46fc39da7bf220a85c4ee38cd99d25

commit 1665a1d16d46fc39da7bf220a85c4ee38cd99d25
Author: msw@chromium.org <msw@chromium.org>
Date: Tue Feb 01 21:16:10 2022

Reland "Make web cursor size limits match on browser and renderer"

This reverts commit 38a8343085e53889eba48fcff78a6c2295927333.

Reason for revert: Fix without regressing ~~https://crbug.com/1292426~~
(Increased WebCursor limit 128->150px to support DevToolsEyeDropper)

Original change's description:
> Revert "Make web cursor size limits match on browser and renderer"
>
> This reverts commit 868b44dd8b4a1a3b9698f561ca17f75e4ec78dd2.
>
> Reason for revert: ~~https://crbug.com/1292426~~
>
> Original change's description:
> > Make web cursor size limits match on browser and renderer
> >
> > Use NSCursor arrowCursor on Mac for ui::mojom::CursorType::kNull.
> > (i.e. when WebCursor is constructed with an overly large custom cursor)
> >
> > ~~Bug: 1246188~~
> > Test: Automated unit tests and WPTs
> > Change-Id: I89627fa13cba96b755b8f80adbc91cfc865b6b1b
> > Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3413912
> > Reviewed-by: Henrique Ferreiro <hferreiro@igalia.com>
> > Reviewed-by: Charlie Harrison <csharrison@chromium.org>
> > Commit-Queue: Mike Wasserman <msw@chromium.org>
> > Auto-Submit: Mike Wasserman <msw@chromium.org>
> > Cr-Commit-Position: refs/heads/main@{#964378}
>
> ~~Bug: 1246188~~
> Change-Id: Id7b3b88e65c012993537ce96c2b5064b7b76646e
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3428347
> Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
> Commit-Queue: Mike Wasserman <msw@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#965475}

~~Fixed: 1246188~~
Bug: 1292426

~~Bug: 1292426~~
Change-Id: I5a490603c3e21e17f3136a3d792a18429eb3f633
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3428624
Auto-Submit: Mike Wasserman <msw@chromium.org>
Reviewed-by: Charlie Harrison <csharrison@chromium.org>
Commit-Queue: Mike Wasserman <msw@chromium.org>
Reviewed-by: Henrique Ferreiro <hferreiro@igalia.com>
Cr-Commit-Position: refs/heads/main@{#965857}

[modify] https://crrev.com/1665a1d16d46fc39da7bf220a85c4ee38cd99d25/content/common/cursors/webcursor_mac.mm
[modify] https://crrev.com/1665a1d16d46fc39da7bf220a85c4ee38cd99d25/content/common/cursors/webcursor.cc
[modify] https://crrev.com/1665a1d16d46fc39da7bf220a85c4ee38cd99d25/content/common/cursors/webcursor_unittest.cc

Comment 29 by amyressler@google.com on Thu, Feb 17, 2022, 6:34 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-2000

*** 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 30 by amyressler@chromium.org on Thu, Feb 17, 2022, 6:58 PM EST Project Member

Congratulations on another one! The VRP Panel has decided to award you $2,000 for this report (which I affectionately refer to as "Mega Cursor"). Thank you for your efforts and reporting this issue to us!

Comment 31 by amyressler@google.com on Fri, Feb 18, 2022, 2:58 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 32 by sheriffbot on Sat, Feb 19, 2022, 2:10 PM EST Project Member

Labels: Merge-NA-100

Not requesting merge to dev (M100) because latest trunk commit (964378) appears to be prior to dev branch point (972766). If this is incorrect, please replace the Merge-NA-100 label with Merge-Request-100. If other changes are required to fix this bug completely, please request a merge if necessary.

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

Comment 33 by alesa...@alesandroortiz.com on Mon, Feb 21, 2022, 7:10 PM EST

Thanks for the reward and for giving the report a great nickname! :)

Comment 34 by amyressler@chromium.org on Mon, Mar 28, 2022, 6:29 PM EDT Project Member

Labels: Release-0-M100

Comment 35 by amyressler@google.com on Tue, Mar 29, 2022, 1:14 PM EDT Project Member

Labels: CVE-2022-1138 CVE_description-missing

Comment 36 by sheriffbot on Wed, May 11, 2022, 1:32 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 37 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 38 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing