Starred by 4 users

Owner: jinsu...@chromium.org

CC: pnoland@chromium.org
adetaylor@chromium.org
twell...@chromium.org
wylieb@chromium.org
jinsu...@chromium.org
fgor...@chromium.org
foolip@chromium.org
amyressler@chromium.org
ender@google.com

Status: Fixed *(Closed)*

Components: UI>Browser>Omnibox
Blink>Fullscreen
UI>Browser>FullScreen

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Android

Pri: 1

Type: Bug-Security

Hotlist-Merge-Review
reward-3000
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
M-98
Target-98
FoundIn-98
Security_Impact-Extended
merge-merged-4896
merge-merged-100
Release-0-M100
CVE-2022-1129

Issue 1300253: Security: Chrome for Android Cancel Enter Fullscreen able to Hide Omnibox

Reported by susah...@gmail.com on Wed, Feb 23, 2022, 2:22 PM EST

Code

When requestFullscreen then canceled by append fullscreen element into <html> element using canvas.toBlob to help achieve appropriate timing, surprisingly the omnibox will be hidden instead of restore to visible state.

VERSION
- Chrome 98.0.4758.101 on Mi 9T; Android 11
- Chrome 98.0.4758.101 on SM-J500F; Android 11
- Chrome Beta 99.0.4844.35 on Mi 9T; Android 11
- Chrome Beta 99.0.4843.35 on SM-J500F; Android 11
- Chrome Beta 99.0.4844.35 on Android Emulator; Android 10 x86_64
- Chrome Dev 100.0.4891.2 on Mi 9T; Android 11
- Chrome Dev 100.0.4891.2 on SM-J500F; Android 11
- Chrome Dev 100.0.4891.2 on Android Emulator; Android 10 x86

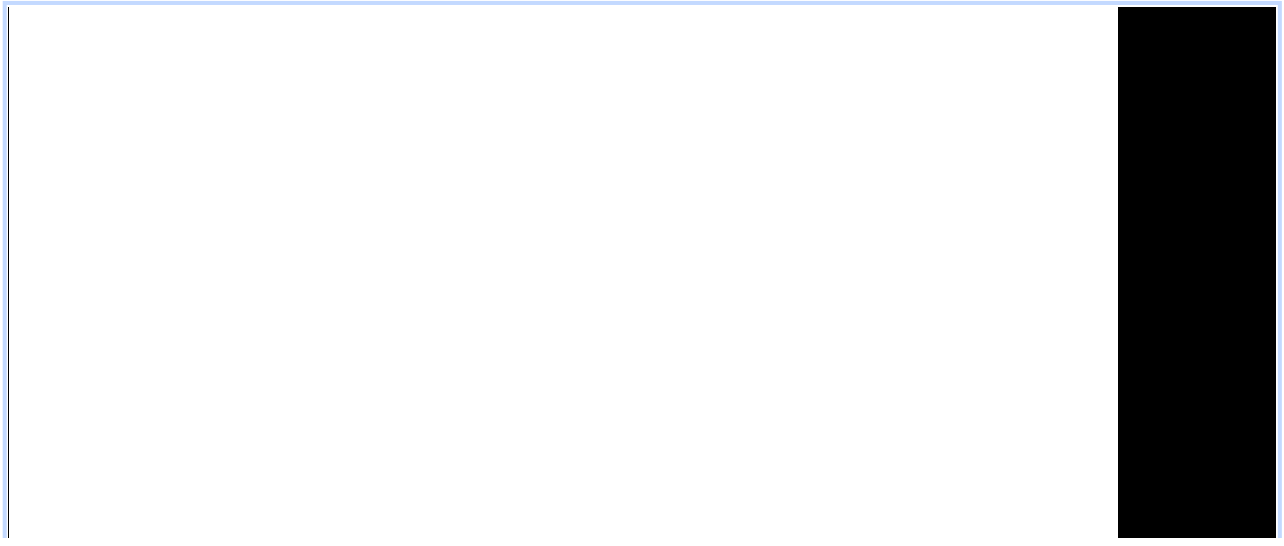
REPRODUCTION CASE
1. Download and extract hideomniboxspoof.zip
2. Open terminal in extract directory
3. Run "python -m http.server 8000"
4. On Chrome for Android visit python webserver ipaddress:8000/iframe.html (i.e. 127.0.0.1:8000/iframe.html)
5. Tap subfolder
6. Tap testcase.html
7. Tap "Tap Here" select element
8. Omnibox will be hidden then spoofed with spoof omnibox.

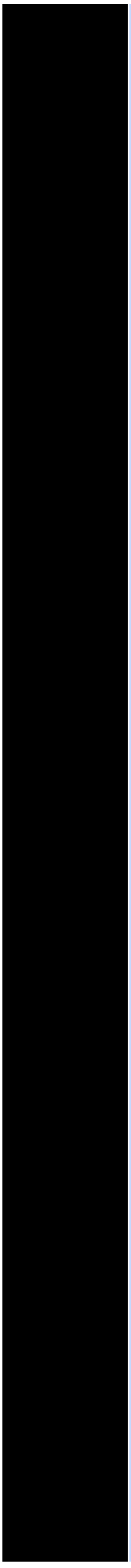
(If omnibox is not hidden as on PoC video, try press back then repeat from step 6)

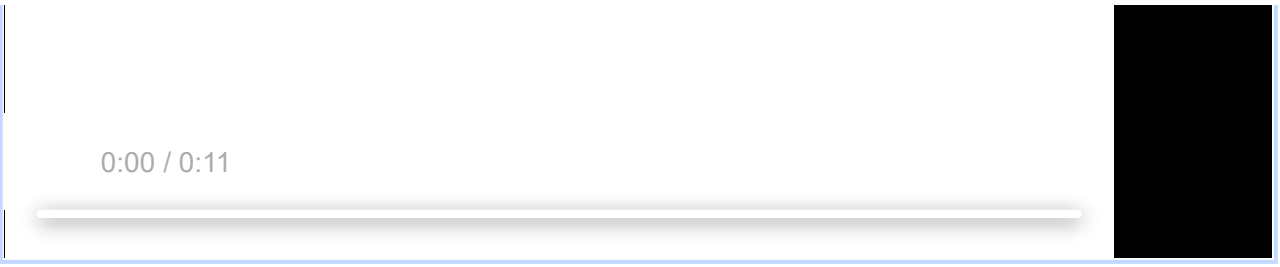
CREDIT INFORMATION
Reporter credit: Irvan Kurniawan (sourc7)

[Deleted] **hideomniboxspoof.zip**

hideomnibox demonstration on Mi 9T.mp4
3.9 MB View Download







Comment 1 by susah...@gmail.com on Wed, Feb 23, 2022, 2:31 PM EST

hideomniboxspoof.zip
14.8 KB Download

Comment 2 by sheriffbot on Wed, Feb 23, 2022, 2:34 PM EST Project Member

Labels: external_security_report

Comment 3 by danakj@chromium.org on Wed, Feb 23, 2022, 3:04 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: foolip@chromium.org
Labels: Security_Severity-High OS-Android Pri-1
Components: UI>Browser>FullScreen Blink>Fullscreen

Unable to repro as I have no android device. => fullscreen owners

Comment 4 by susah...@gmail.com on Wed, Feb 23, 2022, 8:50 PM EST

@danakj @foolip I think we can also cc jinsukkim@chromium.org which previously fixed similar hide omnibox ~~issue 1270593~~

Comment 5 by amyressler@chromium.org on Thu, Mar 3, 2022, 4:38 PM EST Project Member

Cc: jinsu...@chromium.org twell...@chromium.org pnoland@chromium.org wylieb@chromium.org
Components: UI>Browser>Omnibox

Hi jinsukkim@ and twellington@, not sure if foolip@ was the correct owner for this one so cc'ing y'all and others that have recently tackled other fullscreen issues

Comment 6 by amyressler@chromium.org on Thu, Mar 3, 2022, 4:39 PM EST Project Member

Cc: fgor...@chromium.org

adding fgorski@ just in case wrt to omnibox

Comment 7 by twell...@chromium.org on Thu, Mar 3, 2022, 6:29 PM EST Project Member

Owner: jinsu...@chromium.org
Cc: foolip@chromium.org

This seems similar to issue 956338 which was fixed in 97.0.4692.102 by reshowing the omnibox when fullscreen is cancelled.

Jinsuk, do you mind taking this one too?

Comment 8 by jinsu...@chromium.org on Fri, Mar 4, 2022, 11:45 AM EST Project Member

Status: Started (was: Assigned)

Comment 9 by jinsu...@chromium.org on Fri, Mar 4, 2022, 3:37 PM EST Project Member

What this issue has in common with ~~Issue 1270593~~ is that an exit-fullscreen request coming immediately after enter-fullscreen puts Chrome fullscreen state in an inconsistent state.

IUUC, this time fullscreen mode is entered without any problem, but the exit-fullscreen coming too soon somehow prevented LayoutChangeListener[1] for enter-fullscreen from being invoked at all. This turns some internal states (in terms of layout) different from what we see on screen - we're already in fullscreen, but layout height doesn't seem to get updated - it still is a height of normal screen.

Later when exit-fullscreen's own LayoutChangeListener[2] is invoked, it cannot detect any different in layout height and skips |TabBrowserControlsConstraintsHelper.update(mTab, BrowserControlsState.SHOWN, true)|, which makes it fail to show omnibox again.

I haven't figured out graceful ways to fix this. One workaround would be to invoke |TabBrowserControlsConstraintsHelper.update(BrowserControlsState.SHOWN)| at exit-fullscreen always i.e. even if there is not layout height changes. As far as I can tell, we're supposed to restore the omnibox anyway whenever fullscreen mode is exited. https://crrev.com/c/3499699

[1] https://source.chromium.org/chromium/chromium/src/+/main:chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java;l=480;drc=9126f59e3fe456c8bad83424bab74ec514380e79
[2] https://source.chromium.org/chromium/chromium/src/+/main:chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java;l=427;drc=9126f59e3fe456c8bad83424bab74ec514380e79

Comment 10 by fgor...@chromium.org on Fri, Mar 4, 2022, 6:02 PM EST Project Member

Cc: ender@google.com adetaylor@chromium.org

I don't have a good idea. But adding ender and Adrian. (The former to generate ideas with other folks, the latter because I am seeing warnings about security labels).

Comment 11 by adetaylor@chromium.org on Fri, Mar 4, 2022, 6:38 PM EST Project Member

jinsukkim@ fgorski@ with regards to security labels - all we need to know is whether this is a regression introduced since M98 (and if so, which milestone?) or if it's existed before that. Please let me know and I'll add the appropriate labels to get the warnings to go away.

Comment 12 by jinsu...@chromium.org on Fri, Mar 4, 2022, 8:50 PM EST Project Member

I think it has been around for a long time, just waiting to be discovered. So not a regression.

Comment 13 by adetaylor@chromium.org on Sat, Mar 5, 2022, 12:03 AM EST Project Member

Labels: FoundIn-98

Thanks!

Comment 14 by sheriffbot on Sat, Mar 5, 2022, 12:03 AM EST Project Member

Labels: Security_Impact-Extended

Comment 15 by sheriffbot on Sat, Mar 5, 2022, 12:46 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 16 by Git Watcher on Thu, Mar 10, 2022, 6:14 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/37d6456a8fcc12e8719f13470aabf71c7a8ac3cb

commit 37d6456a8fcc12e8719f13470aabf71c7a8ac3cb
Author: Jinsuk Kim <jinsukkim@chromium.org>
Date: Thu Mar 10 23:13:01 2022

Android: Ensure restoring omnibox upon exiting fullscreen mode

The process of enter-fullscreen consists of a few steps which can be stopped in the middle by an immediately following exit-fullscreen event, leaving the internal and visible states inconsistent. This can lead to an incomplete UI when exit-fullscreen request is completed i.e. omnibox is not restored.

This CL triggers omnibox restoration logic when fullscreen state falls in this inconsistent state in which the internal state indicates omnibox is shown, while actually it is not. This can deal with other (yet to be found) cases where the fullscreen end up in a mismatched state. The restoration logic will be a no-op if everything is correct, so does no harm.

~~Bug: 1300253~~
Change-Id: I1a9bc6bec10d11bbb6fbd03866a39e0f96b187fa
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499699
Reviewed-by: Theresa Sullivan <twellington@chromium.org>
Commit-Queue: Jinsuk Kim <jinsukkim@chromium.org>
Cr-Commit-Position: refs/heads/main@{#980005}

[modify]
https://crrev.com/37d6456a8fcc12e8719f13470aabf71c7a8ac3cb/chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java

Comment 17 by xinghuilu@chromium.org on Thu, Mar 17, 2022, 8:31 PM EDT Project Member

Hi, please mark this bug as fixed if all fixes have been landed. Thanks!

Comment 18 by jinsu...@chromium.org on Fri, Mar 18, 2022, 10:07 AM EDT Project Member

Status: Fixed (was: Started)

Comment 19 by sheriffbot on Fri, Mar 18, 2022, 12:41 PM EDT Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Fri, Mar 18, 2022, 1:41 PM EDT Project Member

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

Comment 21 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 (980005) appears to be after extended stable branch point (950365).

Requesting merge to stable M99 because latest trunk commit (980005) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (980005) appears to be after beta branch point (972766).

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

Comment 22 by sheriffbot on Fri, Mar 18, 2022, 2:02 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 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 23 by sheriffbot on Fri, Mar 18, 2022, 2:02 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)

Owners: benmason (Android), harrysouders (iOS), ceb (ChromeOS), ppommana (Desktop)

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

Comment 24 by sheriffbot on Fri, Mar 18, 2022, 2:02 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 25 by jinsu...@chromium.org on Fri, Mar 18, 2022, 2:10 PM EDT Project Member

1. Why does your merge fit within the merge criteria for these milestones?

A patch to a critical security issue

2. What changes specifically would you like to merge? Please link to Gerrit.

https://chromium-review.googlesource.com/c/chromium/src/+/3499699

3. Have the changes been released and tested on canary?

Yes

4. Is this a new feature? If yes, is it behind a Finch flag and are experiments active in any release channels?

No

5. [Chrome OS only]: Was the change reviewed and approved by the Eng Prod Representative?
https://goto.google.com/cros-engprodcomponents

N/A

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.

N/A

Comment 26 by gov...@chromium.org on Fri, Mar 18, 2022, 2:55 PM EDT Project Member

Cc: amyressler@chromium.org

+Amy (Security TPM) for merge review. Thank you.

Comment 27 by amyressler@chromium.org on Fri, Mar 18, 2022, 6:45 PM EDT Project Member

Labels: -Merge-Review-98 -Merge-Review-99 -Merge-Review-100 Merge-Approved-100

M100 merge approved, please merge this fix to branch 4896 NTL 12p PDT, Monday, 21 March so this fix can be included in the M100 stable cut

merge-na M98 and M99 as there are no further planned releases of M99 stable or M98 ES

Comment 28 by Git Watcher on Fri, Mar 18, 2022, 8:52 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/+/56470daf4aa89711328c2476403b468ea8adcc17

commit 56470daf4aa89711328c2476403b468ea8adcc17
Author: Jinsuk Kim <jinsukkim@chromium.org>
Date: Sat Mar 19 00:51:29 2022

Android: Ensure restoring omnibox upon exiting fullscreen mode

The process of enter-fullscreen consists of a few steps which can be
stopped in the middle by an immediately following exit-fullscreen
event, leaving the internal and visible states inconsistent. This
can lead to an incomplete UI when exit-fullscreen request is
completed i.e. omnibox is not restored.

This CL triggers omnibox restoration logic when fullscreen state
falls in this inconsistent state in which the internal state indicates
omnibox is shown, while actually it is not. This can deal with other
(yet to be found) cases where the fullscreen end up in a mismatched
state. The restoration logic will be a no-op if everything is correct,
so does no harm.

(cherry picked from commit 37d6456a8fcc12e8719f13470aabf71c7a8ac3cb)

~~Bug: 1300253~~
Change-Id: I1a9bc6bec10d11bbb6fbd03866a39e0f96b187fa
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3499699
Reviewed-by: Theresa Sullivan <twellington@chromium.org>
Commit-Queue: Jinsuk Kim <jinsukkim@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#980005}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3536637
Auto-Submit: Jinsuk Kim <jinsukkim@chromium.org>
Commit-Queue: Theresa Sullivan <twellington@chromium.org>
Cr-Commit-Position: refs/branch-heads/4896@{#691}

Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]

[modify]
https://crrev.com/56470daf4aa89711328c2476403b468ea8adcc17/chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java

Comment 29 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 30 by amyressler@chromium.org on Wed, Mar 23, 2022, 3:54 PM EDT Project Member

Congratulations, Irvan. The VRP Panel has decided to award you $3,000 for this report. Thank you for your efforts and nice work!

Comment 31 by amyressler@google.com on Fri, Mar 25, 2022, 4:55 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 32 by amyressler@chromium.org on Mon, Mar 28, 2022, 5:54 PM EDT Project Member

Labels: Release-0-M100

Comment 33 by amyressler@google.com on Tue, Mar 29, 2022, 1:13 PM EDT Project Member

Labels: CVE-2022-1129 CVE_description-missing

Comment 34 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 35 by amyressler@google.com on Fri, Jul 22, 2022, 7:36 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 36 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing