Starred by 4 users

Owner:	jinsu...@chromium.org
CC:	twell...@chromium.org tedc...@chromium.org mdjones@chromium.org dcheng@chromium.org amyressler@chromium.org
Status:	Fixed *(Closed)*
Components:	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_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
M-99
Target-99
FoundIn-99
merge-merged-4896
merge-merged-100
Merge-NA-101
Release-2-M100
CVE-2022-1307

Issue 1301873: Security: Chrome for Android Hide Custom Fullscreen Toast View with Repeated Exit Enter Fullscreen Request

Reported by susah...@gmail.com on Mon, Feb 28, 2022, 11:48 PM EST

Code

VULNERABILITY DETAILS

After ~~issue 1264561~~ Chrome on Android fullscreen toast now migrated from native Android toast framework to custom toast view.

Normally the custom toast view will be displayed for 5 seconds, interestingly with appropriate timing I found the custom toast view able to hide quickly (only displayed less than a second) and there a chance to not showing at all by using repeated exit then enter fullscreen request.

Furthermore when custom toast view hide earlier, we can combine with showing Android native framework e.g. HTML5 select dropdown, the dropdown will appear in top of custom toast view, so user won't see the toast at all.

VERSION

I able to reproduce the hide toast early on following Chrome version and device:
- Chrome Beta 99.0.4844.44 on Mi 9T; Android 11
- Chrome Beta 99.0.4844.44 on SM-J500F; Android 11
- Chrome Beta 99.0.4844.44 on Android Emulator; Android 10 x86_64
- Chrome Dev 100.0.4896.12 on Mi 9T; Android 11
- Chrome Dev 100.0.4896.12 on SM-J500F; Android 11
- Chrome Dev 100.0.4896.12 on Redmi Note 9 Pro; Android 11

REPRODUCTION CASE

1. Download and extract hidecustomtoast.zip
2. Open terminal in extract directory
3. Run "node app.js" to serve the web server
4. Visit the web server ipaddress:8000 (i.e. 127.0.0.1:8000)
5. Tap "Tap Here" select element
6. Android select dropdown appear in top of custom toast view, then after interact with select dropdown the custom toast view no longer visible (as it was hidden earlier)

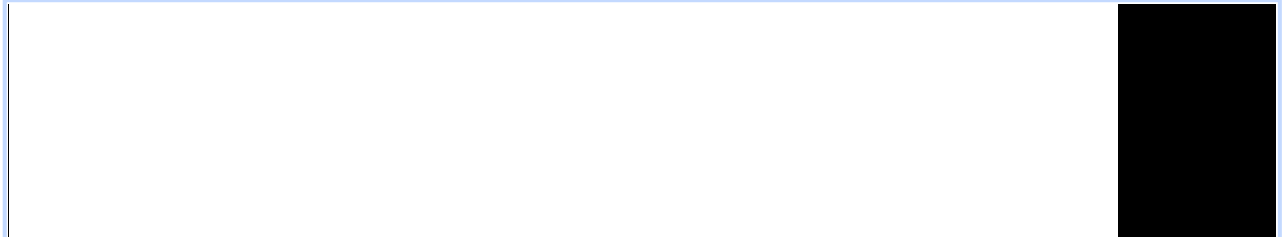
(Sometimes the select dropdown not appear as on PoC video, try to reload the page then try again from step 5)

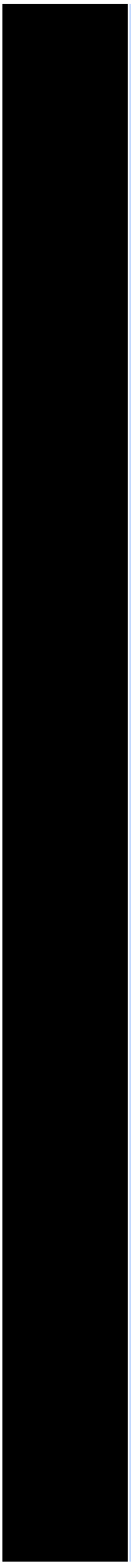
CREDIT INFORMATION

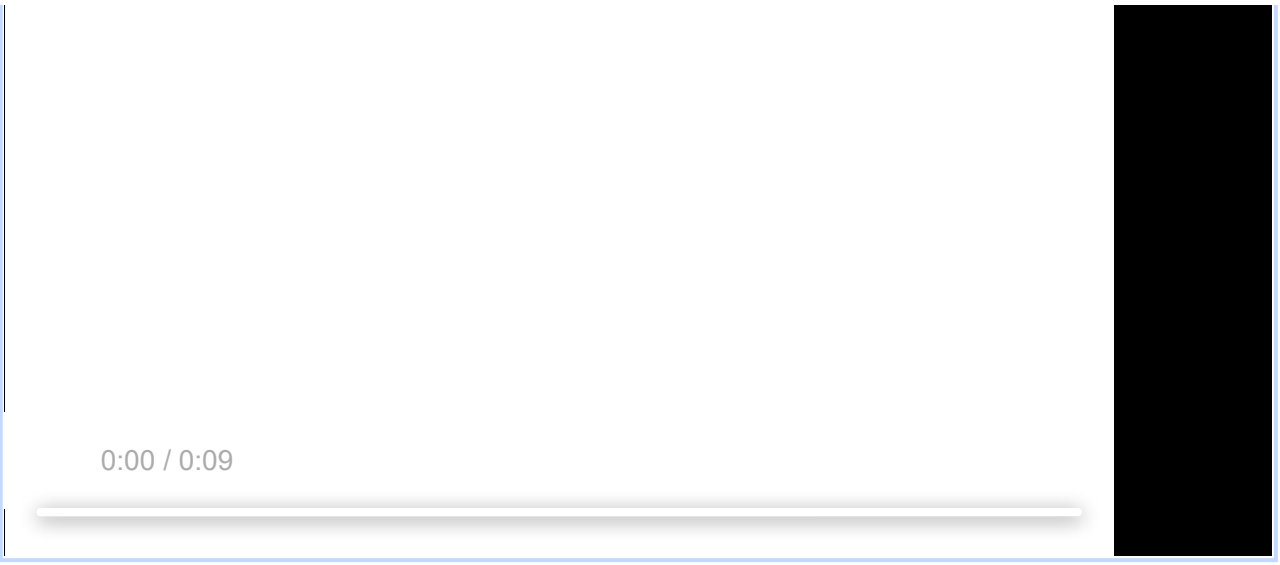
Reporter credit: Irvan Kurniawan (sourc7)

hidecustomtoast.zip
628 KB Download

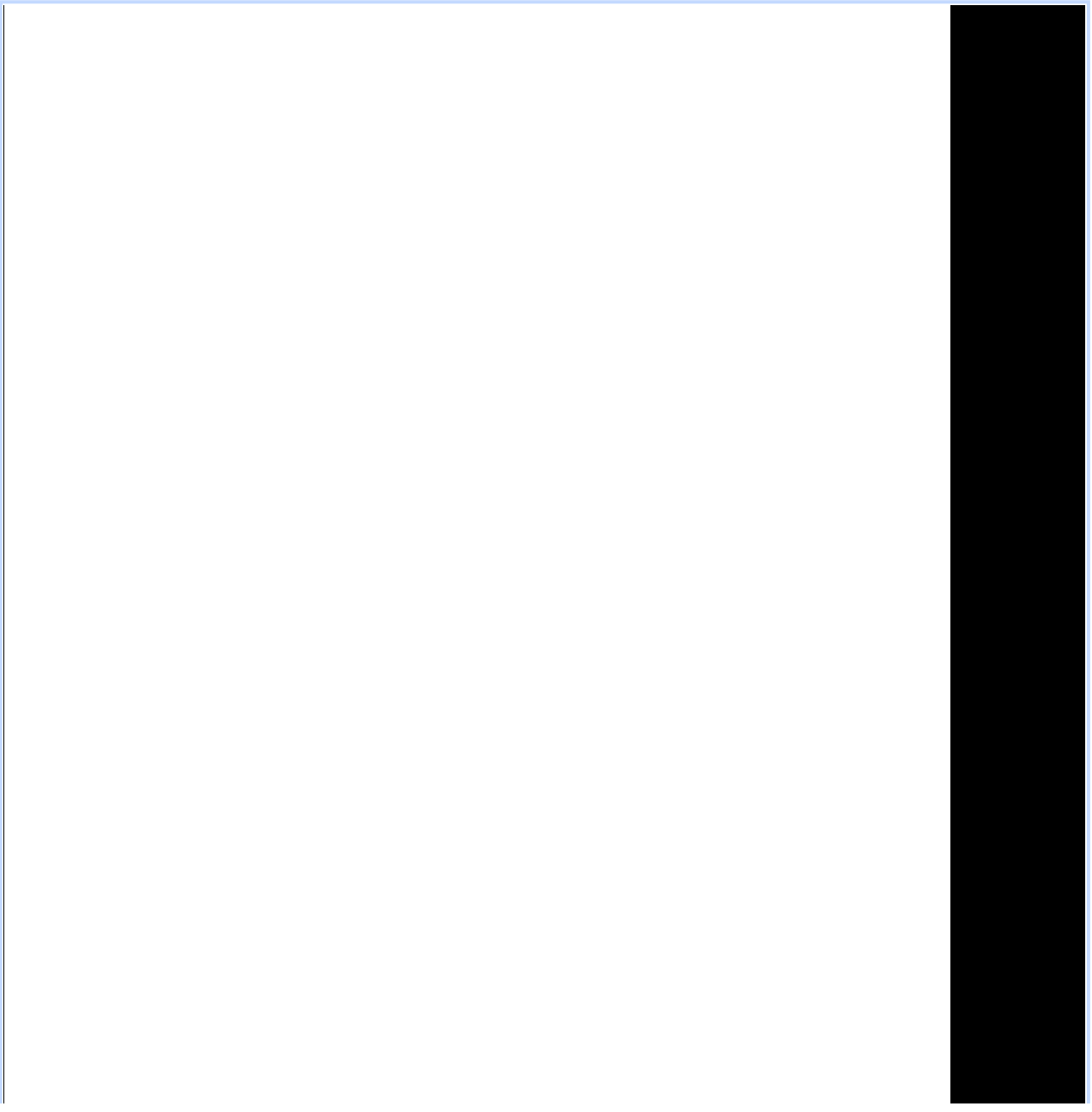
hidecustomtoast + select dropdown on Mi 9T.mp4
277 KB View Download

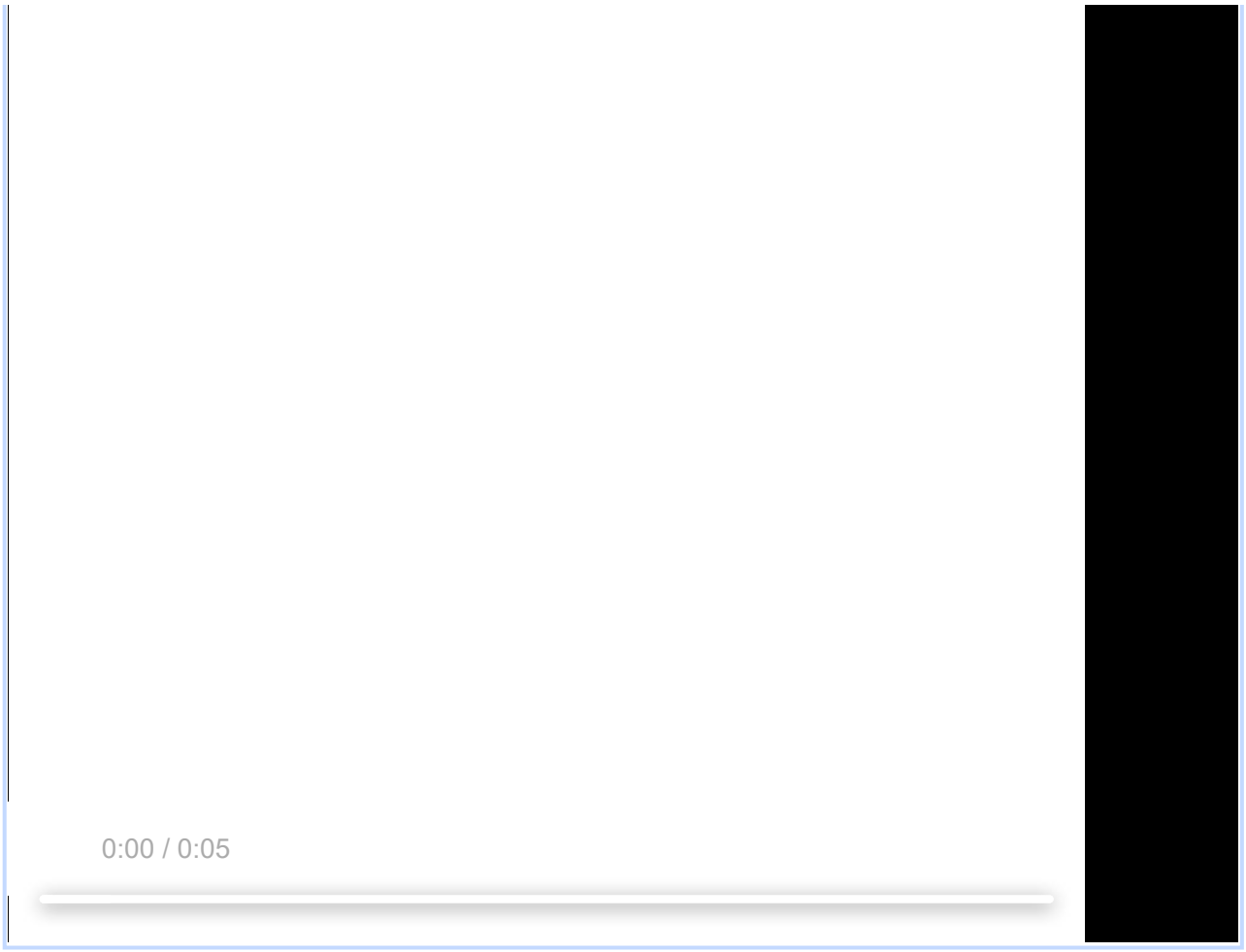






hidecustomtoast + select dropdown on Android Emulator.webm
1.5 MB View Download





Comment 1 by sheriffbot on Mon, Feb 28, 2022, 11:52 PM EST Project Member

Labels: external_security_report

Comment 2 by dcheng@chromium.org on Wed, Mar 2, 2022, 9:20 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: jinsu...@chromium.org
Cc: twell...@chromium.org tedc...@chromium.org
Labels: FoundIn-99 Security_Severity-High OS-Android Pri-1
Components: UI>Browser>FullScreen

I've attached test case from the zip file directly. I was able to reproduce (though flakily) without the delays from the sync XHRs. The repro might be more stable with the sync XHRs, but I didn't want to run NodeJS :)

+jinsukkim, do you mind taking a look at this or do you know who would be able to take a closer look at this?

I'm going to tag this one as High severity, as this allows a page to "impersonate other origins". There is somewhat of a mitigating factor with the select box popping up, but I think it'd be possible to integrate that in a way that fit naturally and wouldn't be overly suspicious to a user.

testcase.html
1.2 KB View Download

Comment 3 by twell...@chromium.org on Wed, Mar 2, 2022, 9:26 PM EST Project Member

Cc: dcheng@chromium.org

The custom toast was added originally to address a "medium" severity security ~~issue 1264561~~. If this is "high" severity, should we rollback and reland w/ consideration for this case as well?

Comment 4 by sheriffbot on Wed, Mar 2, 2022, 9:29 PM EST Project Member

Labels: Security_Impact-Stable

Comment 5 by jinsu...@chromium.org on Thu, Mar 3, 2022, 11:56 AM EST Project Member

Status: Started (was: Assigned)

FYI a similar case has been reported (~~Issue 1270052~~) this issue is more complicated as it combines multiple xhr fullscreen requests and select dropdown.

Comment 6 by sheriffbot on Thu, Mar 3, 2022, 12:47 PM EST Project Member

Labels: M-99 Target-99

Setting milestone and target because of high severity.

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

Comment 7 by jinsu...@chromium.org on Thu, Mar 3, 2022, 7:02 PM EST Project Member

Cc: mdjones@chromium.org

Here's what happened when you have enter/exit/enterFullscreen in succession:
- For the first enterFullscreen, a toast is displayed
- ExitFullscreen removes the toast but not immediately (i.e. after fade out animation).
- Another EnterFullscreen now creates a new toast, but animation finish callback above now gets executed to remove the current toast.

In order to prevent this, we need to cancel the attempt to remove the toast initiated by the previous exitFullscreen. This can be addressed by 1) exitFullscreen posts a runnable hiding the toast rather than calling it directly 2) at the beginning of enterFullscreen we remove any hide-toast runnable in the queue.

Comment 8 by Git Watcher on Thu, Mar 10, 2022, 11:01 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/5326b6967d000c677efa23b9f849145b0b06df07

commit 5326b6967d000c677efa23b9f849145b0b06df07
Author: Jinsuk Kim <jinsukkim@chromium.org>
Date: Fri Mar 11 04:00:06 2022

Android: Ensure the fullscreen toast lasts long enough

For exit/enter fullscreen events coming in back to back, the attempt
to remove the toast for the preceding exit event can accidentally
delete the following fullscreen toast in display. This CL cancels
the fade-out animation of the toast before showing a new one to
prevent the current toast from being interfered.

~~Bug: 1301873~~

Change-Id: I4d604f93a9a458e182d76b22af8ab4661a6104cb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501458
Reviewed-by: Matthew Jones <mdjones@chromium.org>

Reviewed-by: Matthew Jones <mdjones@chromium.org>
Reviewed-by: Theresa Sullivan <twellington@chromium.org>
Commit-Queue: Jinsuk Kim <jinsukkim@chromium.org>
Cr-Commit-Position: refs/heads/main@{#980123}

[modify]
https://crrev.com/5326b6967d000c677efa23b9f849145b0b06df07/chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java

Comment 9 by adetaylor@google.com on Thu, Mar 24, 2022, 6:58 PM EDT Project Member

jinsukkim@ is this Fixed, or is there more work to do? If it's fixed please mark it as such, and then Sheriffbot will add appropriate merge requests.

Comment 10 by jinsu...@chromium.org on Thu, Mar 24, 2022, 7:12 PM EDT Project Member

Status: Fixed (was: Started)

Comment 11 by sheriffbot on Sun, Mar 27, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 12 by sheriffbot on Sun, Mar 27, 2022, 1:40 PM EDT Project Member

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

Comment 13 by sheriffbot on Sun, Mar 27, 2022, 2:06 PM EDT Project Member

Labels: Merge-NA-101 Merge-Request-100 Merge-Request-99

Requesting merge to stable M99 because latest trunk commit (980123) appears to be after stable branch point (961656).

Requesting merge to beta M100 because latest trunk commit (980123) appears to be after beta branch point (972766).

Not requesting merge to dev (M101) because latest trunk commit (980123) appears to be prior to dev branch point (982481). If this is incorrect, please replace the Merge-NA-101 label with Merge-Request-101. 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 14 by sheriffbot on Sun, Mar 27, 2022, 2:10 PM EDT Project Member

Labels: -Merge-Request-100 Hotlist-Merge-Review Merge-Review-100

Merge review required: M100 has already been cut for stable release.

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 15 by sheriffbot on Sun, Mar 27, 2022, 2:10 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 16 by amyressler@chromium.org on Thu, Mar 31, 2022, 3:50 PM EDT Project Member

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

M100 merge approved, please merge this fix to branch 4896 at your earliest convenience -- thank you!

Comment 17 by amyressler@google.com on Thu, Mar 31, 2022, 5:14 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 18 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:17 PM EDT Project Member

Congratulations, Irvan! The VRP Panel has decided to award you $3000 for this report. Thank you for your efforts and reporting this issue to us!

Comment 19 by amyressler@google.com on Fri, Apr 1, 2022, 4:08 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 20 by sheriffbot on Tue, Apr 5, 2022, 12:21 PM EDT Project Member

Cc: amyressler@chromium.org

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 21 by gov...@chromium.org on Wed, Apr 6, 2022, 5:47 PM EDT Project Member

Please merge your change to M100 branch 4896 by Thursday, 04/07 3:00 PM PT so it can be included in next week's respin. Thank you.

Comment 22 by Git Watcher on Wed, Apr 6, 2022, 8:03 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/+/c682acd05ebd33c6fb89ee409984559374f3e436

commit c682acd05ebd33c6fb89ee409984559374f3e436
Author: Jinsuk Kim <jinsukkim@chromium.org>
Date: Thu Apr 07 00:02:50 2022

Android: Ensure the fullscreen toast lasts long enough

For exit/enter fullscreen events coming in back to back, the attempt
to remove the toast for the preceding exit event can accidentally
delete the following fullscreen toast in display. This CL cancels
the fade-out animation of the toast before showing a new one to
prevent the current toast from being interfered.

(cherry picked from commit 5326b6967d000c677efa23b9f849145b0b06df07)

~~Bug: 1301873~~
Change-Id: I4d604f93a9a458e182d76b22af8ab4661a6104cb
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3501458
Reviewed-by: Matthew Jones <mdjones@chromium.org>
Reviewed-by: Theresa Sullivan <twellington@chromium.org>
Commit-Queue: Jinsuk Kim <jinsukkim@chromium.org>
Cr-Original-Commit-Position: refs/heads/main@{#980123}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3574792
Cr-Commit-Position: refs/branch-heads/4896@{#1061}
Cr-Branched-From: 1f63ff4bc27570761b35ffbc7f938f6586f7bee8-refs/heads/main@{#972766}

[modify]
https://crrev.com/c682acd05ebd33c6fb89ee409984559374f3e436/chrome/android/java/src/org/chromium/chrome/browser/fullscreen/FullscreenHtmlApiHandler.java

fullscreen/FullscreenHtmlApiHandler.java

Comment 23 by adetaylor@google.com on Mon, Apr 11, 2022, 1:15 PM EDT Project Member

Labels: Release-2-M100

Comment 24 by adetaylor@google.com on Mon, Apr 11, 2022, 1:29 PM EDT Project Member

Labels: CVE-2022-1307 CVE_description-missing

Comment 25 by sheriffbot on Fri, Jul 1, 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 26 by amyressler@google.com on Tue, Jul 26, 2022, 4:57 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 27 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing