☆ Starred by 2 users

Owner:	a...@chromium.org
CC:	cthomp@chromium.org mea...@chromium.org mas...@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>FullScreen Blink>WindowDialog
Modified:	Jun 11, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Chrome, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Reward-1000
Security_Impact-Stable
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
M-89
Target-88
Target-89
merge-merged-4240
merge-merged-86
LTR-Merged-86
LTS-Security-86
Release-0-M89
external_security_report
merge-merged-4389
merge-merged-89
CVE-2021-21176

Issue 1170584: UI/URL Spoofing by putting the page into fullscreen when a user opens the emoji dialog

Reported by herre...@gmail.com on Mon, Jan 25, 2021, 7:39 PM EST

Code

VULNERABILITY DETAILS
By waiting for a user to open the emoji dialog and at the same time forcing them to enter into fullscreen it is possible to overlap the fullscreen warning message and then perform UI/URL spoofing.

The attack works as follows:
1. User accesses attacker's website and right-clicks on an input field to make the context menu show up.
2. As soon as the context menu opens, the input field is moved up (to align it directly above where the fullscreen warning message is supposed to appear).
3. When the user selects the emoji option, the script forces the victim to enter fullscreen, which places the emoji dialog above the fullscreen warning message, hiding it.
4. The hidden fullscreen message will disappear after around 5 seconds, and later, when the user eventually closes the dialog, the message will be long gone and the page will remain spoofed.

This allows an effect similar to the UI/URL spoofing of ~~Bug 550017~~.

Here's an unlisted video demonstrating the issue:
https://youtu.be/vdgtNchq7gQ

VERSION
Chrome Version: 88.0.4324.104 (Official Build) (64-bit)
Operating System: Windows 10

REPRODUCTION CASE
1. Access https://lbherrera.github.io/lab/emoji-spoof/index.html
2. Right-click on the input field and select the "Emoji" option.
3. The page will enter into fullscreen and the message warning the user will be overlayed by the emoji dialog.

CREDIT INFORMATION
Reporter credit: Luan Herrera (@lbherrera_)

index.html
1.2 KB View Download

Comment 1 by sheriffbot on Mon, Jan 25, 2021, 7:43 PM EST Project Member
Labels: external_security_report

Comment 2 by vakh@chromium.org on Mon, Jan 25, 2021, 8:41 PM EST Project Member
Thanks for the report. I'll triage this bug. Please take the POC off Github so it isn't publicly accessible.

Comment 3 by vakh@chromium.org on Mon, Jan 25, 2021, 8:46 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: a...@chromium.org
Cc: mea...@chromium.org cthomp@chromium.org
Labels: Security_Severity-Medium Security_Impact-Stable
Components: UI>Browser>FullScreen Blink>WindowDialog

avi@, meacer@, cthomp@ -- between you three, one of you is probably the right owner. Please feel free to triage further as appropriate.

Comment 4 by vakh@chromium.org on Mon, Jan 25, 2021, 8:47 PM EST Project Member

Labels: OS-Chrome OS-Linux OS-Mac OS-Windows Pri-2

Note that the "full screen" notification does appear momentarily before the emoji dialog appears on top of that.

Comment 5 by cthomp@chromium.org on Mon, Jan 25, 2021, 8:56 PM EST Project Member

Seems plausible that we need to add the fullscreen block for the emoji dialog (like avi@ did for permissions dialogs and protocol handlers in crrev.com/c/2041871 and crrev.com/c/2044658). Unfortunately this doesn't look as straightforward as those cases, as I think the emoji dialog is a one-shot trigger to an OS-specific command rather than something we can easily track the lifetime of inside Chrome [1].

[1] https://source.chromium.org/chromium/chromium/src/+/master:ui/base/emoji/emoji_panel_helper.h;bpv=1;bpt=1

Comment 6 by a...@chromium.org on Mon, Jan 25, 2021, 9:03 PM EST Project Member

I cannot repro on the Mac; your PoC does a fullscreen trigger with keycode 91, which is not how context menus work on the Mac. Note also that the fullscreen bubble on the Mac is explicitly coded to show z-ordered over _every_ window, including the emoji palette, so I would be surprised if this could be made to work on the Mac.

Which platforms have you reproduced this on?

Comment 7 by herre...@gmail.com on Mon, Jan 25, 2021, 9:38 PM EST

#2: The PoC is not public, it was hosted on a private repository and is served through GitHub Pages (access happens only through the full path), but I have removed the PoC as recommended.

#6: The PoC was only tested on Windows 10.

Comment 8 by sheriffbot on Tue, Jan 26, 2021, 1:05 PM EST Project Member

Labels: Target-88 M-88

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 9 by sheriffbot on Tue, Jan 26, 2021, 1:41 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 10 by a...@chromium.org on Tue, Feb 2, 2021, 6:57 PM EST Project Member

As per comment 5, “Seems plausible that we need to add the fullscreen block for the emoji dialog” I will attempt to do so.

Comment 11 by bugdroid on Wed, Feb 3, 2021, 9:13 PM EST Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/f8ab2f2363d4b08a75c1db76b5031c70858a3e5e

commit f8ab2f2363d4b08a75c1db76b5031c70858a3e5e
Author: Avi Drissman <avi@chromium.org>
Date: Thu Feb 04 02:12:56 2021

Drop fullscreen on invocation of the emoji dialog

The emoji dialog can be used to interfere with the fullscreen
bubble, so drop fullscreen.

~~Fixed: 1170584~~
Change-Id: I8acc69c7d41971e5f55a65528169ff57ab410e7a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2669847
Reviewed-by: Chris Thompson <cthomp@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Commit-Position: refs/heads/master@{#850406}

[modify] https://crrev.com/f8ab2f2363d4b08a75c1db76b5031c70858a3e5e/chrome/browser/renderer_context_menu/render_view_context_menu.cc

Comment 12 by sheriffbot on Thu, Feb 4, 2021, 12:44 PM EST Project Member

Labels: reward-topanel

Comment 13 by sheriffbot on Thu, Feb 4, 2021, 1:58 PM EST Project Member

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

Comment 14 by sheriffbot on Thu, Feb 4, 2021, 2:24 PM EST Project Member

Labels: Merge-Request-89

Requesting merge to beta M89 because latest trunk commit (850406) appears to be after beta branch point (843830).

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

Comment 15 by sheriffbot on Thu, Feb 4, 2021, 9:14 PM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89's targeted beta branch promotion date has already passed, so this requires manual review
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://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- 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 ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

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

Comment 16 by pbommana@google.com on Mon, Feb 8, 2021, 12:40 AM EST Project Member

avi@ request to provide answers to questions from comment#15

Comment 17 by a...@chromium.org on Mon, Feb 8, 2021, 11:51 AM EST Project Member

OP, the fix landed in 90.0.4409.0. Can you confirm that this no longer reproduces?

Comment 18 by herre...@gmail.com on Mon, Feb 8, 2021, 12:11 PM EST

#17: I can confirm the PoC no longer reproduces in 90.0.4412.0.

Comment 19 by a...@chromium.org on Mon, Feb 8, 2021, 12:19 PM EST Project Member

1. Yes, it is a security fix.
2. https://chromium-review.googlesource.com/c/chromium/src/+/2669847
3. Yes.
4. No.
5. Security fix.
6. No.
7. n/a

Comment 20 by adetaylor@google.com on Mon, Feb 8, 2021, 7:33 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389.

Comment 21 by bugdroid on Mon, Feb 8, 2021, 10:11 PM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/15e7b81e4b0fd0aae3fc48e85d1232d9651ba24a

commit 15e7b81e4b0fd0aae3fc48e85d1232d9651ba24a
Author: Avi Drissman <avi@chromium.org>
Date: Tue Feb 09 03:09:13 2021

Drop fullscreen on invocation of the emoji dialog

The emoji dialog can be used to interfere with the fullscreen
bubble, so drop fullscreen.

(cherry picked from commit f8ab2f2363d4b08a75c1db76b5031c70858a3e5e)

~~Fixed: 1170584~~
Change-Id: I8acc69c7d41971e5f55a65528169ff57ab410e7a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2669847
Reviewed-by: Chris Thompson <cthomp@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#850406}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2682859
Auto-Submit: Avi Drissman <avi@chromium.org>
Commit-Queue: Chris Thompson <cthomp@chromium.org>
Cr-Commit-Position: refs/branch-heads/4389@{#829}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/15e7b81e4b0fd0aae3fc48e85d1232d9651ba24a/chrome/browser/renderer_context_menu/render_view_context_menu.cc

Comment 22 by herre...@gmail.com on Mon, Feb 22, 2021, 11:23 AM EST

Hi, any updates regarding the panel decision for this issue? Thanks!

Comment 23 by adetaylor@google.com on Fri, Feb 26, 2021, 1:00 PM EST Project Member

Apologies, the panel has currently got quite a backlog of low and medium severity bugs. It hasn't been overlooked.

Comment 24 by adetaylor@google.com on Fri, Feb 26, 2021, 1:08 PM EST Project Member

Labels: Release-0-M89

Comment 25 by adetaylor@google.com on Mon, Mar 1, 2021, 7:28 PM EST Project Member

Labels: CVE-2021-21176 CVE_description-missing

Comment 26 by vsavu@google.com on Wed, Mar 3, 2021, 5:11 AM EST Project Member

Labels: LTS-Merge-Request-86

Comment 27 by vsavu@google.com on Wed, Mar 3, 2021, 6:00 AM EST Project Member

Labels: LTS-Security-86

Comment 28 by gianluca@google.com on Wed, Mar 3, 2021, 10:34 AM EST Project Member

Labels: LTS-Merge-Approved-86

Comment 29 by sheriffbot on Wed, Mar 3, 2021, 12:21 PM EST Project Member

Labels: -M-88 Target-89 M-89

Comment 30 by amyressler@google.com on Wed, Mar 3, 2021, 7:34 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 31 by amyressler@google.com on Wed, Mar 3, 2021, 8:21 PM EST Project Member

Congratulations, Luan! The VRP Panel has decided to award you $1,000 for this report. Thank you and nice work!

Comment 32 by vsavu@google.com on Thu, Mar 4, 2021, 8:43 AM EST Project Member

Labels: -LTS-Merge-Approved-86 -LTS-Merge-Request-86 LTR-Merged-86

Comment 33 by Git Watcher on Thu, Mar 4, 2021, 9:00 AM EST Project Member

Labels: merge-merged-4240 merge-merged-86

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/d98209611dc951a7c4ec2d00c299f993d4234769

```
commit d98209611dc951a7c4ec2d00c299f993d4234769
Author: Avi Drissman <avi@chromium.org>
Date: Thu Mar 04 13:59:56 2021

Drop fullscreen on invocation of the emoji dialog

The emoji dialog can be used to interfere with the fullscreen
bubble, so drop fullscreen.

(cherry picked from commit f8ab2f2363d4b08a75c1db76b5031c70858a3e5e)

~~Fixed: 1170584~~
Change-Id: I8acc69c7d41971e5f55a65528169ff57ab410e7a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2669847
Reviewed-by: Chris Thompson <cthomp@chromium.org>
Commit-Queue: Avi Drissman <avi@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#850406}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2731510
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1557}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/d98209611dc951a7c4ec2d00c299f993d4234769/chrome/browser/renderer_context_menu/render_view_context_menu.cc
```

Comment 34 by amyressler@google.com on Fri, Mar 5, 2021, 11:03 AM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 35 by amyressler@google.com on Tue, Mar 9, 2021, 12:58 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 36 by sheriffbot on Fri, Jun 11, 2021, 1:51 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