☆ Starred by 3 users

Owner:	mamir@chromium.org
CC:	kerenzhu@google.com pbos@chromium.org adetaylor@chromium.org avi@google.com bsep@chromium.org sky@chromium.org schwering@google.com est...@chromium.org dfried@google.com dfried@chromium.org amyressler@chromium.org mamir@chromium.org koerber@google.com battre@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill>UI
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

reward-3000
Security_Severity-Medium
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
Target-94
M-94
FoundIn-92
Security_Impact-Extended
Release-0-M97
CVE-2022-0110

Issue 1237310: Security: Autofill prompt can render over permission prompts after they have opened

Reported by alesa...@alesandroortiz.com on Thu, Aug 5, 2021, 10:41 PM EDT

Code

VULNERABILITY DETAILS

Pages with carefully-positioned input fields can cause the browser to render autofill prompts over certain browser UI elements, such as permission prompts and probably other persistent browser UI elements.

After the ~~issue 1235222~~ fix (currently only in Canary), overlap is only possible in the content area, however this is sufficient to cover sensitive areas of permission prompts and potentially other browser UI elements. In PoC 1, we cover either the prompt text or the "Block" button depending on whether the bookmarks bar is shown.
Without that fix, overlap is also possible over the bookmarks bar and omnibar, which allows for more complete spoofs. Since the fix is only in Canary, this is currently possible in Stable. In PoC 2, we cover the omnibar and prompt text, which allows for complete UI origin spoof.

The PoCs also use secondary techniques described in ~~issue 1172533~~:
1. Add arbitrary autofill entries via iframes containing forms.
2. Persist autofill prompt by adding event listeners for most events and cancelling any received events + changing the input element type from `text` to `button`.

VERSION

92.0.4515.107 (Official Build) (64-bit) (cohort: Stable), 94.0.4598.2 Canary (only content area spoof in Canary due to ~~issue 1235222~~ fix)
Windows 10 OS Version 2009 (Build 19042.1110)

REPRODUCTION CASE

See attached video with recording of all PoCs.

PoC 1a: Content area spoof, with bookmarks bar (default browser configuration)
1. With bookmarks bar shown, navigate to https://alesandroortiz.com/security/chromium/autofill-ui-permission.html
2. Double-click anywhere in page.

PoC 1b: Content area spoof, no bookmarks bar (non-default browser configuration)
1. With bookmarks bar *not* shown, navigate to https://alesandroortiz.com/security/chromium/autofill-ui-permission.html
2. Double-click anywhere in page.

PoC 2: Complete spoof (won't work in Canary)
1. Navigate to https://alesandroortiz.com/security/chromium/autofill-ui-permission-omnibar.html
2. Double-click anywhere in page.

For all PoCs:
Observed: Autofill prompt is rendered above permission prompts.
Expected: Autofill prompt is not rendered if position overlaps with permission prompts.

Please note that if the mitigation leads to the autofill prompt being rendered below the permission prompt, it could result in another security vulnerability. The new behavior might allow for effective autofill prompt hiding, which could be used to trick user into autofilling form without their awareness. Therefore only rendering one at a time is expected, but not both

simultaneously.

CREDIT INFORMATION

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

autofill-ui-permission.html
5.1 KB View Download

autofill-ui-permission-omnibar.html
4.3 KB View Download

autofill-setup-frame.html
830 bytes View Download

autofill-ui-permission.mp4
1.2 MB View Download

Comment 1 by sheriffbot on Thu, Aug 5, 2021, 10:43 PM EDT Project Member

Labels: external_security_report

Comment 2 by kenrb@chromium.org on Fri, Aug 6, 2021, 11:12 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: mamir@chromium.org
Labels: Security_Severity-Medium FoundIn-94 OS-Chrome OS-Linux OS-Mac OS-Windows Pri-1
Components: UI>Browser>Autofill>UI

mamir@: Thanks for looking at the previous issues in this area so promptly. Would you mind having a look at this one as well?

Comment 3 by sheriffbot on Fri, Aug 6, 2021, 11:15 PM EDT Project Member

Labels: Security_Impact-Head

Comment 4 by alesa...@alesandroortiz.com on Fri, Aug 6, 2021, 11:21 PM EDT

Security impact should be Stable, not Head, since it does repro on Stable as well.

Comment 5 by sheriffbot on Sat, Aug 7, 2021, 12:55 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 Sat, Aug 7, 2021, 1:01 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 7 by mamir@chromium.org on Mon, Aug 9, 2021, 3:53 AM EDT Project Member

Cc: schwering@google.com koerber@google.com

Comment 8 by mamir@chromium.org on Mon, Aug 9, 2021, 6:50 AM EDT Project Member

Labels: Needs-Feedback

Thank you for reporting this one.

This bug should have been fixed already in
https://chromium-review.googlesource.com/c/chromium/src/+/2953407
which made to Beta channel and will be out M93.

@reporter: are you able to repro this on *Beta* and report back if it reproducible?

Comment 9 by alesa...@alesandroortiz.com on Mon, Aug 9, 2021, 12:53 PM EDT

Yes, able to repro on 93.0.4577.25 Beta, 94.0.4600.0 Canary, plus 92.0.4515.131 Stable.

Comment 10 by mamir@chromium.org on Tue, Aug 10, 2021, 8:32 AM EDT Project Member

Labels: -ReleaseBlock-Stable

@reporter: thank you very much for testing it again.

together with schwering@, we have looked into this:

1- This is more or less the same as ~~crbug.com/1204722~~
2- It looks like the fix in ~~crbug.com/1204722~~ works for both Linux and Mac but not for Windows.
3- This isn't a regression and hence I am removing the Stable Release block label. (introduce in c#6)

3- This isn't a regression and hence I am removing the Stable Release block label. (introduce in c#6)
4- I will start working on finding a fix for this on Windows.

Thank you

Comment 11 by alesa...@alesandroortiz.com on Tue, Aug 10, 2021, 11:09 AM EDT

Thanks for the triage! When you have a chance, please also update the Security_Impact and FoundIn labels, since this repros on 92.x Stable (labels indicate 94.x Head).

Comment 12 by sheriffbot on Tue, Aug 10, 2021, 12:57 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 13 by mamir@chromium.org on Tue, Aug 10, 2021, 2:15 PM EDT Project Member

Labels: -Needs-Feedback -Security_Impact-Head -ReleaseBlock-Stable -FoundIn-94 FoundIn-92 Security_Impact-Stable

Comment 14 by mamir@chromium.org on Mon, Aug 16, 2021, 6:49 AM EDT Project Member

Labels: -OS-Linux -OS-Chrome -OS-Mac

Comment 15 by sheriffbot on Mon, Aug 16, 2021, 1:12 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 16 by sheriffbot on Mon, Aug 30, 2021, 12:21 PM EDT Project Member

mamir: 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 17 by mamir@chromium.org on Mon, Sep 6, 2021, 4:03 PM EDT Project Member

Cc: sky@chromium.org est...@chromium.org

(+sky@ in case he can chime in, and also he will mostly review the fix when I find one)
(+estade@ as an FYI)

The reason for the behavioral change on Windows is the NativeWidgetType [1]

For Linux, it is NATIVE_WIDGET_AURA, while on Windows version Vista or newer [2], the native type is

For Linux, it is NATIVE_WIDGET_AURA, while on Windows version Vista or newer [2], the native type is DESKTOP_NATIVE_WIDGET_AURA.

NativeWidgetType decides [1] the hierarchy of the widgets and hence, when it's set to DESKTOP_NATIVE_WIDGET_AURA, the prompts aren't children widgets of the browser frame, and hence the check in [3] cannot detect them.

I don't have a Windows machine with Windows version before Vista to test that, but the issue should *not* repro on version before Vista.

I am still looking for a mitigation for this issue on Vista+ Windows versions.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/native_widget_factory.cc;l=27;drc=ac3b649031d4c82cb66e26144551e2b38363065b

[2]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/chrome_views_delegate_win.cc;l=146;drc=ac3b649031d4c82cb66e26144551e2b38363065b

[3]
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/ui/views/autofill/autofill_popup_view_utils.cc;l=114;drc=c373e6393f376de7d3203a15dbfc3de80318c488

Comment 18 by mamir@chromium.org on Tue, Sep 7, 2021, 4:56 AM EDT Project Member

Cc: bsep@chromium.org

Comment 19 by sky@chromium.org on Tue, Sep 7, 2021, 1:53 PM EDT Project Member

I would expect Widget::GetAllOwnedWidgets() to include widgets that are backed by DesktopNativeWidgetAura. Have you tried it?

Comment 20 by mamir@chromium.org on Wed, Sep 8, 2021, 10:51 AM EDT Project Member

Thanks Scott!
I have tried Widget::GetAllOwnedWidgets() and it doesn't return anything more than Widget::GetAllChildWidgets()

IIUC, GetAllOwnedWidgets() returns all transient children in addition to the actual children native widgets.
When I audit the method TransientWindowManager::AddTransientChild() [1], it's actually *never* called. Do you think this is a bug? I cannot easily tell which code path should have added the transit children.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:ui/wm/core/transient_window_manager.cc;l=60;drc=c48ea0ec9f1390319579700d542248dc7b2b70dc

Comment 21 by mamir@chromium.org on Wed, Sep 8, 2021, 4:50 PM EDT Project Member

Cc: dfried@chromium.org

Comment 22 by mamir@chromium.org on Wed, Sep 8, 2021, 4:52 PM EDT Project Member

Cc: dfried@google.com

Comment 23 by dfried@google.com on Wed, Sep 8, 2021, 5:19 PM EDT Project Member

Vote to use Z-order to make sure the tab permissions dialog is higher-precedence than the web page:
https://source.chromium.org/chromium/chromium/src/+/main:ui/base/ui_base_types.h;l=51

Ping me on DM if you need help setting this up.

As a fallback, as we discussed, we could assign an ElementIdentifier to the permissions bubble and use ElementTracker plus the existing code to detect the presence of that bubble and actively avoid it.

Comment 24 by mamir@chromium.org on Wed, Sep 8, 2021, 5:59 PM EDT Project Member

Cc: kerenzhu@google.com

Comment 25 by mamir@chromium.org on Thu, Sep 9, 2021, 3:06 AM EDT Project Member

Cc: avi@google.com

Adding more context from chat with Chrome Desktop UI

Avi Drissman:
"
Only the Mac supports all these different values for the z-order

so on Windows, all the z orders that are not “normal” are equally “in front”

The "security" option has no effect on windows.

Windows and Linux only have two window z orders

normal and “always on top”

so for those platforms, all the non-normal levels get collapsed to “always on top”
"

This all matches what I recall when I first worked on ~~crbug.com/1204722~~.

Given how complicated this is, the only possible solution that doesn't involve changing the whole parenting system of Widgets would be to specifically track the permission prompt using ElementTracker as recommended in c#23

Comment 26 by sheriffbot on Thu, Sep 23, 2021, 12:22 PM EDT Project Member

mamir: 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 27 by mamir@chromium.org on Thu, Sep 23, 2021, 12:39 PM EDT Project Member

This is on my radar, and will prepare the CL that uses ElementTracker to detect permissions prompt in Windows.

Comment 28 by alesa...@alesandroortiz.com on Thu, Oct 7, 2021, 1:39 PM EDT

The original ~~issue 1204722~~ was made public a few minutes ago. Can someone restrict its visibility given it still repros in Windows as reported in this bug?

Comment 29 by mamir@chromium.org on Mon, Oct 18, 2021, 4:07 AM EDT Project Member

Cc: amyressler@chromium.org adetaylor@chromium.org mamir@chromium.org

~~Issue 1259174~~ has been merged into this issue.

Comment 30 by mamir@chromium.org on Thu, Oct 21, 2021, 3:08 PM EDT Project Member

Cc: pbos@chromium.org

Comment 31 by Git Watcher on Fri, Oct 29, 2021, 4:29 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/33a92473a985268c5a1623e7cbe1a027d4b3520a

commit 33a92473a985268c5a1623e7cbe1a027d4b3520a
Author: Mohamed Amir Yosef <mamir@chromium.org>
Date: Fri Oct 29 20:28:32 2021

[Autofill] Don't show Autofill dropdown if overlaps with permissions

This CL makes sure that the Autofill dropdown isn't opened if it will
overlap with an open permissions prompt.

~~Bug: 1237310~~
Change-Id: I6882e39af13168a0fa5f82338430ec362c7ff015
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3236729
Reviewed-by: Dana Fried <dfried@chromium.org>
Commit-Queue: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Commit-Position: refs/heads/main@{#936535}

[modify]
https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/autofill/autofill_popup_view_utils.h
[modify]
https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/permission_bubble/permission_prompt_bubble_view.h
[modify]
https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/autofill/autofill_popup_view_native_views.cc
[modify]
https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/permission_bubble/permission_prompt_bubble_view.cc
[modify]
https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/autofill/autofill_popup_view_

https://crrev.com/33a92473a985268c5a1623e7cbe1a027d4b3520a/chrome/browser/ui/views/autofill/autofill_popup_view_utils.cc

Comment 32 by mamir@chromium.org on Fri, Oct 29, 2021, 4:34 PM EDT Project Member

Status: Fixed (was: Assigned)

Comment 33 by sheriffbot on Sat, Oct 30, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 34 by sheriffbot on Sat, Oct 30, 2021, 1:41 PM EDT Project Member

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

Comment 35 by mamir@chromium.org on Tue, Nov 2, 2021, 8:28 AM EDT Project Member

Status: Verified (was: Fixed)

Comment 36 by mamir@chromium.org on Tue, Nov 2, 2021, 8:29 AM EDT Project Member

Status: Fixed (was: Verified)

Comment 37 by amyressler@google.com on Wed, Nov 3, 2021, 1:53 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 38 by amyressler@chromium.org on Wed, Nov 3, 2021, 2:21 PM EDT Project Member

Congratulations, Alesandro! The VRP Panel has decided to award you $3000 for this report. Nice work!

Comment 39 by amyressler@google.com on Thu, Nov 4, 2021, 4:32 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 40 by alesa...@alesandroortiz.com on Thu, Nov 11, 2021, 6:54 PM EST

Thanks for the reward!

I've verified as fixed (for the permission prompt) in 98.0.4700.0 Canary on Windows 10 Version 20H2 (Build 19042.1288)

Comment 41 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:33 PM EST Project Member

Labels: Release-0-M97

Comment 42 by amyressler@google.com on Tue, Jan 4, 2022, 1:34 PM EST Project Member

Labels: CVE-2022-0110 CVE_description-missing

Comment 43 by sheriffbot on Sat, Feb 5, 2022, 1:29 PM EST 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 44 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted