Starred by 2 users

Owner:	gtanzer@chromium.org
CC:	a...@chromium.org csharrison@chromium.org suzhang@google.com mustaq@chromium.org shivanisha@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>PopupBlocker Blink>Input
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac, Fuchsia, Lacros
Pri:	1
Type:	Bug-Security

Security_Severity-Medium
allpublic
CVE_description-submitted
M-98
Target-96
Target-98
FoundIn-94
Security_Impact-Extended
Release-0-M101
CVE-2022-1497

Blocking:	Issue 1123606 ~~Issue 1291210~~ ~~Issue 1314768~~

Issue 1264543: Security: Popup with noopener does not consume user activation

Reported by abalq...@microsoft.com on Thu, Oct 28, 2021, 3:42 PM EDT

Code

VULNERABILITY DETAILS

When opening a popup window using the 'noopener' directive it seems like it does not consume user gesture which leads to spoofing content in cross origin websites.

VERSION

Chrome Version: 97.0.4684.2 (Official Build) canary (64-bit)
Operating System: Windows 11

REPRODUCTION CASE

Open attached PoC and click on the button 'Using noopener' you should see datalist values appear. Without 'noopener' it does not work.

This can be modified to achieve the same bug as ~~Bug 1204722~~.

See attached screenshot for what it looks like.

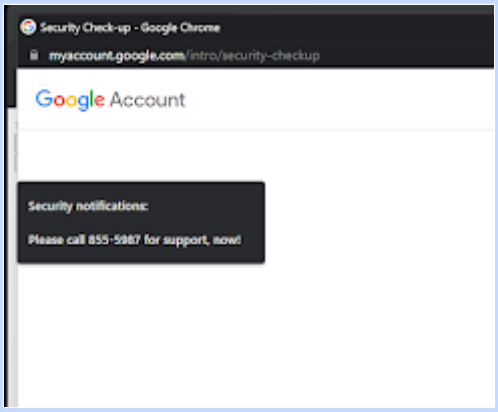
I am not sure why this only works when the popup has 'noopener', maybe some logic is missing for this edge case.

CREDIT INFORMATION

Reporter credit: Abdulrahman Alqabandi, Microsoft Browser Vulnerability Research

pops.html
858 bytes View Download

noopener.png
17.2 KB View Download



Comment 1 by danakj@chromium.org on Wed, Nov 3, 2021, 9:30 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: mustaq@chromium.org

Labels: Security_Severity-Medium OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Mac OS-Windows OS-Lacros Pri-2
Components: Blink>Input

It's a bit flaky - sometimes the popup shows, sometimes the dropdown does, but only one of the two for "without noopener". And also a bit flaky for "with noopener" but I can see that both do appear sometimes.

This is on 95.0.4638.54 Linux.

Comment 2 by mustaq@chromium.org on Wed, Nov 3, 2021, 11:04 AM EDT Project Member

I can repro the bug. I think it appears flaky only because a transparent textbox is on top of the second button (so it is hard to click the button itself). Here is a more precise way to repro:

A. Click on the first button.
This opens the popup AND the datalist associated to the transparent textbox. The datalist opens because of the textbox is focused through JS. This programmatic focusing works because user activation is not consumed by the popup. This is the bug.

B. Click on the second button outside the hidden textbox. Check mouse pointer for a clue: the "arrow cursor" appears only near the top/left inside-edge of the button.
This opens the popup, but not the datalist because programmatic focusing into the textbox fails because of lack of user activation (consumed by the popup). This is WAI.

C. Click on the hidden textbox above the second button, when the mouse cursor turns to "I-beam".
The datalist opens because the textbox is manually focused with user activation. This is WAI.

Comment 3 by mustaq@chromium.org on Wed, Nov 3, 2021, 11:29 AM EDT Project Member

Summary: Security: Popup with noopener does not consume user activation (was: Security: Popup with noopener can be used to spoof content cross origin using datalist dropdown)
Cc: a...@chromium.org csharrison@chromium.org
Components: UI>Browser>PopupBlocker

Here is a minimal repro:
https://codepen.io/mustaqahmed/pen/porprBP

avi@: Do you know why we don't consume user activation in this special case? Is it a recent change? Should this bug be a P1?

Comment 4 by a...@chromium.org on Wed, Nov 3, 2021, 12:34 PM EDT Project Member

I don't know of any reason why we would want to have this be a special case, and don't know why it is.

Comment 5 by danakj@chromium.org on Thu, Nov 4, 2021, 1:16 PM EDT Project Member

Labels: FoundIn-94 Pri-1

Re: P1. You're right. My understanding of https://chromium.googlesource.com/chromium/src/+/master/docs/security/severity-guidelines.md is this is a Medium, which should be >= P1.

I was able to repro with your codepen in M94 as well

Comment 6 by sheriffbot on Thu, Nov 4, 2021, 1:19 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 7 by sheriffbot on Fri, Nov 5, 2021, 12:52 PM EDT Project Member

Labels: Target-96 M-96

Setting milestone and target because of medium severity.

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

Comment 8 by sheriffbot on Wed, Nov 17, 2021, 12:21 PM EST Project Member

mustaq: 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 9 by sheriffbot on Mon, Nov 29, 2021, 11:10 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 10 by mustaq@chromium.org on Mon, Nov 29, 2021, 11:17 AM EST Project Member

Leaving the priority as P1, we agreed about it in #c5.

I will try to find out the root cause this week.

Comment 11 by sheriffbot on Thu, Dec 30, 2021, 11:11 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 12 by sheriffbot on Mon, Jan 10, 2022, 11:11 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 13 by sheriffbot on Thu, Jan 20, 2022, 11:11 AM EST Project Member

This issue hasn't been updated in the last 30 days - please update it or consider lowering its priority.

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 14 by mustaq@chromium.org on Thu, Jan 27, 2022, 11:29 AM EST Project Member

Cc: shivanisha@chromium.org gtanzer@chromium.org

Comment 15 by gtanzer@chromium.org on Thu, Jan 27, 2022, 11:39 AM EST Project Member

This turns out to be the root cause of 1291210, because we recently made fenced frames use noopener.

For what it's worth, if you try to open multiple popups in quick succession, it seems to get caught by the popup blocker anyway. (That's not to say there aren't other ways it could be exploited.)

```
button = document.createElement('button');
button.innerHTML="Click me";
document.body.appendChild(button);
button.addEventListener('click', () => { for (let i = 0; i < 10; i++)
{ window.open('about:blank', '_blank', 'noopener'); } console.log("navigator.userActivation.isActive: " +
navigator.userActivation.isActive)});
```

Comment 16 by gtanzer@chromium.org on Thu, Jan 27, 2022, 11:42 AM EST Project Member

Blocking: 1291210

Comment 17 by sheriffbot on Wed, Feb 2, 2022, 12:22 PM EST Project Member

Labels: -M-96 M-98 Target-98

Comment 18 by gtanzer@chromium.org on Mon, Feb 14, 2022, 1:08 PM EST Project Member

Blocking: 1123606

Comment 19 by mustaq@chromium.org on Tue, Feb 15, 2022, 11:43 AM EST Project Member

Thanks gtanzer@ for your offer to look into this!

I would have been unavailable for this for a few more weeks!

Comment 20 by mustaq@chromium.org on Tue, Feb 15, 2022, 11:43 AM EST Project Member

Owner: gtanzer@chromium.org
Cc: -gtanzer@chromium.org mustaq@chromium.org

Comment 21 by gtanzer@chromium.org on Thu, Feb 17, 2022, 11:25 AM EST Project Member

Status: Started (was: Assigned)

Comment 22 by Git Watcher on Tue, Feb 22, 2022, 3:12 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d

commit e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d
Author: Garrett Tanzer <gtanzer@chromium.org>
Date: Tue Feb 22 20:11:51 2022

Fix noopener case for user activation consumption

The flow for user activation consumption in window.open was as follows:

Renderer: ask the browser to create a new window
Browser: consume transient user activation (in the browser, and via RPC to remote frames only)
Browser: return success for opener, return ignore for noopener
Renderer: consume transient user activation upon success

So in the noopener case, the renderer with the local frame where the window.open originated didn't have its transient user activation consumed.

The new behavior is to consume user activation in the calling renderer whenever it is consumed in the browser. We accomplish this by returning a distinct value kBlocked to represent failure before the browser consumes user activation.

~~Bug: 1264543~~, ~~1291210~~
Change-Id: Iffb6e3fd772bef625d3d28e600e6fb73d70ab29f
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3468171
Reviewed-by: Dominic Farolino <dom@chromium.org>
Reviewed-by: Ken Buchanan <kenrb@chromium.org>
Reviewed-by: Mustaq Ahmed <mustaq@chromium.org>
Reviewed-by: Charles Reis <creis@chromium.org>
Reviewed-by: Jonathan Ross <jonross@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Garrett Tanzer <gtanzer@chromium.org>
Cr-Commit-Position: refs/heads/main@{#973876}

[add] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/third_party/blink/web_tests/wpt_internal/fenced_frame/restrict-size.https.html
[modify] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/content/renderer/render_view_impl.cc
[modify] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/content/common/frame.mojom
[modify] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/content/browser/renderer_host/render_frame_host_impl.cc
[modify] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/third_party/blink/web_tests/wpt_internal/fenced_frame/consume-user-activation.https.html
[modify] https://crrev.com/e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d/chrome/browser/site_isolation/chrome_site_per_process_browsertest.cc

Comment 23 by gtanzer@chromium.org on Tue, Feb 22, 2022, 3:14 PM EST Project Member

Status: Fixed (was: Started)

Comment 24 by Git Watcher on Tue, Feb 22, 2022, 7:18 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/361ec38044f34036d920350a72557a51de0ed157

commit 361ec38044f34036d920350a72557a51de0ed157
Author: Dana Fried <dfried@google.com>
Date: Wed Feb 23 00:17:36 2022

Revert "Fix noopener case for user activation consumption"

This reverts commit e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d.

~~Bug: 1300002~~
Reason for revert: Likely cause for UAF in MSAN test

Original change's description:
> Fix noopener case for user activation consumption
>
>
> The flow for user activation consumption in window.open was as follows:
>
> Renderer: ask the browser to create a new window
> Browser: consume transient user activation (in the browser, and via RPC
> to remote frames only)
> Browser: return success for opener, return ignore for noopener
> Renderer: consume transient user activation upon success
>
> So in the noopener case, the renderer with the local frame where the
> window.open originated didn't have its transient user activation
> consumed.
>
>
> The new behavior is to consume user activation in the calling renderer
> whenever it is consumed in the browser. We accomplish this by returning
> a distinct value kBlocked to represent failure before the browser
> consumes user activation.
>
> ~~Bug: 1264543~~, ~~1291210~~
> Change-Id: Iffb6e3fd772bef625d3d28e600e6fb73d70ab29f
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3468171
> Reviewed-by: Dominic Farolino <dom@chromium.org>
> Reviewed-by: Ken Buchanan <kenrb@chromium.org>
> Reviewed-by: Mustaq Ahmed <mustaq@chromium.org>
> Reviewed-by: Charles Reis <creis@chromium.org>
> Reviewed-by: Jonathan Ross <jonross@chromium.org>
> Reviewed-by: Daniel Cheng <dcheng@chromium.org>
> Commit-Queue: Garrett Tanzer <gtanzer@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#973876}

~~Bug: 1264543~~, ~~1291210~~
Change-Id: Ieee4eaee4b57b618cf7773a60c73e1dafa82aba7
No-Presubmit: true
No-Tree-Checks: true
No-Try: true
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3482601
Owners-Override: Dana Fried <dfried@google.com>
Auto-Submit: Dana Fried <dfried@google.com>
Commit-Queue: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Cr-Commit-Position: refs/heads/main@{#973980}

[delete]
https://crrev.com/be69096ac259b71011e29b6bf95c9eb1f7d7a897/third_party/blink/web_tests/wpt_internal/fenced_frame/restrict-size.https.html
[modify] https://crrev.com/361ec38044f34036d920350a72557a51de0ed157/content/renderer/render_view_impl.cc
[modify] https://crrev.com/361ec38044f34036d920350a72557a51de0ed157/content/common/frame.mojom
[modify]
https://crrev.com/361ec38044f34036d920350a72557a51de0ed157/content/browser/renderer_host/render_frame_host_impl.cc
[modify]
https://crrev.com/361ec38044f34036d920350a72557a51de0ed157/chrome/browser/site_isolation/chrome_site_per_process_browsertest.cc
[modify]
https://crrev.com/361ec38044f34036d920350a72557a51de0ed157/third_party/blink/web_tests/wpt_internal/fenced_frame/consume-user-activation.https.html

Comment 25 by mustaq@chromium.org on Wed, Feb 23, 2022, 1:39 PM EST Project Member

Status: Assigned (was: Fixed)

Reopening until the reland happens.

Comment 26 by Git Watcher on Wed, Mar 2, 2022, 1:34 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/6b66a45021a0eef9795568b1f5797968723f381b

commit 6b66a45021a0eef9795568b1f5797968723f381b
Author: Garrett Tanzer <gtanzer@chromium.org>
Date: Wed Mar 02 18:33:42 2022

Reland "Fix noopener case for user activation consumption"

This is a reland of e9828a82b5c182dc9a7fb0ae7226c35ba1726e7d

The MSAN error is from checking status before err in
content/renderer/render_view_impl.cc .
https://ci.chromium.org/ui/p/chromium/builders/ci/Linux%20ChromiumOS%20MSan%20Tests/b8821495655905086193/overview

The fix is to split the check for err and kIgnore into two checks,

and put the err check before kBlocked.

It is probably possible for the browser to consume user activation

it is probably possible for the browser to consume user activation
but then eventually mojo returns an error and the renderer doesn't
consume activation, but that seems pretty marginal.

Original change's description:
> Fix noopener case for user activation consumption
>
>
> The flow for user activation consumption in window.open was as follows:
>
> Renderer: ask the browser to create a new window
> Browser: consume transient user activation (in the browser, and via RPC
> to remote frames only)
> Browser: return success for opener, return ignore for noopener
> Renderer: consume transient user activation upon success
>
> So in the noopener case, the renderer with the local frame where the
> window.open originated didn't have its transient user activation
> consumed.
>
>
> The new behavior is to consume user activation in the calling renderer
> whenever it is consumed in the browser. We accomplish this by returning
> a distinct value kBlocked to represent failure before the browser
> consumes user activation.
>
> ~~Bug: 1264543~~, ~~1291210~~
> Change-Id: Iffb6e3fd772bef625d3d28e600e6fb73d70ab29f
> Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3468171
> Reviewed-by: Dominic Farolino <dom@chromium.org>
> Reviewed-by: Ken Buchanan <kenrb@chromium.org>
> Reviewed-by: Mustaq Ahmed <mustaq@chromium.org>
> Reviewed-by: Charles Reis <creis@chromium.org>
> Reviewed-by: Jonathan Ross <jonross@chromium.org>
> Reviewed-by: Daniel Cheng <dcheng@chromium.org>
> Commit-Queue: Garrett Tanzer <gtanzer@chromium.org>
> Cr-Commit-Position: refs/heads/main@{#973876}

~~Bug: 1264543~~, ~~1291210~~
Change-Id: Ie27c4d68db34dfd98adee7cc5c743953dad59834
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3481666
Reviewed-by: Jonathan Ross <jonross@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Reviewed-by: Mustaq Ahmed <mustaq@chromium.org>
Reviewed-by: Ken Buchanan <kenrb@chromium.org>
Reviewed-by: Charles Reis <creis@chromium.org>
Commit-Queue: Garrett Tanzer <gtanzer@chromium.org>
Cr-Commit-Position: refs/heads/main@{#976745}

[add]
https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/third_party/blink/web_tests/wpt_internal/fenced_frame/restrict-size.https.html
[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/content/renderer/render_view_impl.cc
[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/content/common/frame.mojom

[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/content/common/frame.mojom
[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/content/browser/renderer_host/render_frame_host_impl.cc
[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/third_party/blink/web_tests/wpt_internal/fenced_frame/consume-user-activation.https.html
[modify] https://crrev.com/6b66a45021a0eef9795568b1f5797968723f381b/chrome/browser/site_isolation/chrome_site_per_process_browsertest.cc

Comment 27 by gtanzer@chromium.org on Wed, Mar 2, 2022, 1:51 PM EST Project Member

Status: Fixed (was: Assigned)

Hopefully the reland will stick.

Comment 28 by sheriffbot on Thu, Mar 3, 2022, 1:40 PM EST Project Member

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

Comment 29 by mustaq@chromium.org on Mon, Apr 11, 2022, 10:20 AM EDT Project Member

Blocking: 1314768

Comment 30 by mustaq@google.com on Tue, Apr 12, 2022, 2:22 PM EDT Project Member

Cc: suzhang@google.com

Comment 31 by amyressler@chromium.org on Mon, Apr 25, 2022, 8:57 PM EDT Project Member

Labels: Release-0-M101

Comment 32 by amyressler@google.com on Tue, Apr 26, 2022, 4:32 PM EDT Project Member

Labels: CVE-2022-1497 CVE_description-missing

Comment 33 by sheriffbot on Thu, Jun 9, 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 34 by alesa...@alesandroortiz.com on Thu, Jun 9, 2022, 2:01 PM EDT

As an informative note, while this issue probably had other impacts (such as opening multiple popups?), the PoC (autofill over different-origin popup) seems similar to ~~issue 1239760~~, which only seemed to reproduce on Windows and had more limited impacts. That issue had a separate fix: https://bugs.chromium.org/p/chromium/issues/detail?id=1239760#c27

I think that ~~issue 1239760~~'s fix also fixed this issue's specific PoC, since the fix was for all platforms. Worth noting that ~~issue 1239760~~ did not depend on noopener, so this issue's fix probably would have not fixed the other issue.

Comment 35 by amyressler@google.com on Tue, Jul 26, 2022, 5:37 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