Starred by 3 users

Owner:	mho...@microsoft.com
CC:	mho...@microsoft.com cthomp@chromium.org c...@chromium.org abalq...@microsoft.com mgiuca@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebShare
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	2
Type:	Bug-Security

Reward-1000
Security_Severity-Low
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-92
Security_Impact-Extended
Release-0-M97
CVE-2022-0118

Issue 1238631: Security: Share dialog on Windows can render over address bar, window controls

Reported by alesa...@alesandroortiz.com on Tue, Aug 10, 2021, 11:51 PM EDT

Code

VULNERABILITY DETAILS

The navigator.share() dialog on Windows can be shown over sensitive browser UI, such as the address bar and window controls, in short windows. A malicious page can effectively trick a user into thinking the shared items (text, URL, files) are coming from a different origin, based on address bar origin and page contents of the visible background window, combined with the lack of browser UI or window controls in the popup window.

This may also occur in other OSes, but I have not tested them.

Code analysis indicates this is a system dialog initiated by Chrome. Hopefully there's a way for Chrome to tell the OS to show the dialog below sensitive browser UI such as the address bar. Alternatively, Chrome could avoid opening the dialog when the window is shorter than a safe threshold.

https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/webshare/win/share_operation.cc;l=424;drc=7ef1cfdc609b6c5515a604c5f75ec5d45da2872f
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/webshare/win/show_share_ui_for_window_operation.cc;l=140;drc=e308547f071951c559ac93814733aa04a31c4e1d

ADDITIONAL CONTEXT

Adding origin information in the share dialog may help make the initiator clear to the user, both for security and usability purposes. Currently, even when used as intended, the initiator can be a mystery to the user. On Windows, the UI design looks like part of the OS or a non-Chrome application, therefore web origin information might be particularly important to prevent OS/app spoofing of some sort. Unsure how feasible this is, given the dialog seems to be implemented by the OS. Also unsure how this varies across OSes.

(I accidentally discovered the share dialog after an errant click in an embedded YouTube video; didn't think it was initiated by a website or Chrome, especially since UI design is from Windows, not Chrome. Initially thought I accidentally used a Windows keyboard shortcut that tried to share who-knows-what.)

VERSION

Chrome Version: 92.0.4515.131 (Official Build) (64-bit) (cohort: Stable), 94.0.4603.1 Canary
Operating System: Windows 10 OS Version 2009 (Build 19042.1110)

REPRODUCTION CASE

1. Navigate to https://alesandroortiz.com/security/chromium/share-shortwin.html
2. Double-click anywhere in page.

Observed: Share dialog is shown over address bar, window controls.
Expected: Share dialog is shown below address bar and other sensitive browser UI.

Note: Under certain circumstances, the second click on the popup is not necessary due to issue 1085982 (security restricted). This allows for more effective spoofing.

A more plausible attack could be showing this over drive[.]google[.]com or another origin where sharing files might be more

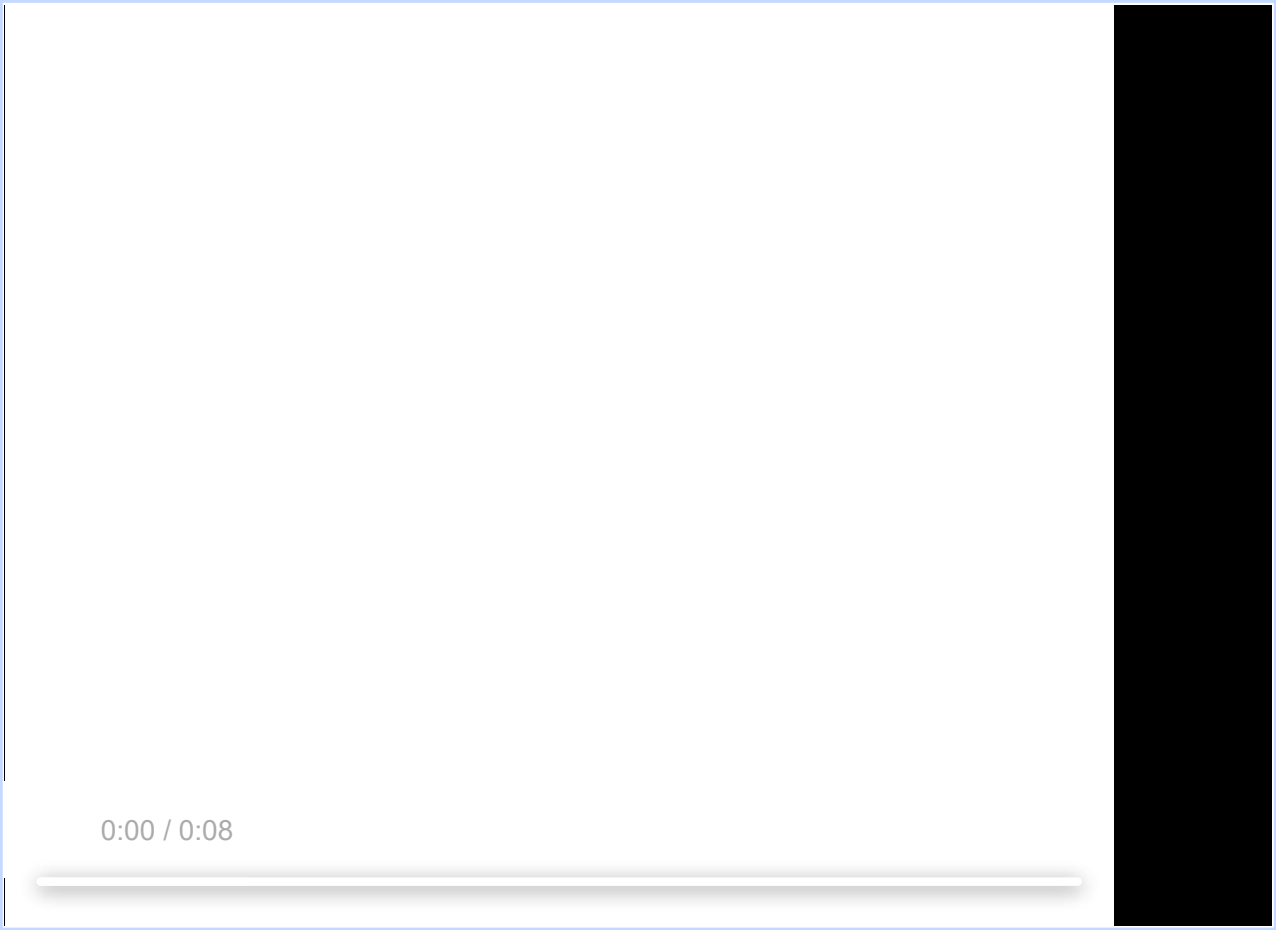
expected by user.

CREDIT INFORMATION

CREDIT INFORMATION

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

share-shortwin.mp4
920 KB View Download



share-shortwin.html
1.0 KB View Download

share-shortwin-popup.html
326 bytes View Download

Comment 1 by sheriffbot on Tue, Aug 10, 2021, 11:53 PM EDT Project Member

Labels: external_security_report

Comment 2 by wfh@chromium.org on Wed, Aug 11, 2021, 6:23 PM EDT Project Member

Status: Available (was: Unconfirmed)
Labels: Security_Severity-Low FoundIn-92 Security_Impact-Stable OS-Windows Pri-1
Components: UI>Browser>Sharing

Thanks for your report. This does look similar to your other recent reports e.g. ~~issue 1235222~~.

Comment 3 by alesa...@alesandroortiz.com on Wed, Aug 11, 2021, 6:52 PM EDT

Thanks for initial triage.

I'm exploring different ways to cover browser UI with other browser UIs, so expect a few more reports around this theme

I'm exploring different ways to cover browser UI with other browser UIs, so expect a few more reports around this theme but using different features (and requiring different fixes).

Got inspired to focus on this by recently disclosed reports (mainly ~~issue 1172533~~) and this blog post:
https://microsoftedge.github.io/edgevr/posts/ui-security-thinking-outside-the-viewport/

Comment 4 by wfh@chromium.org on Wed, Aug 11, 2021, 6:53 PM EDT Project Member

Status: Assigned (was: Available)
Owner: ericwilligers@chromium.org
Cc: cthomp@chromium.org
Components: -UI>Browser>Sharing Blink>WebShare

[assign to correct component] ericwilligers can you take a look at this bug? Is it possible for us to represent the origin in the dialog somehow?

Comment 5 by ericwilligers@chromium.org on Wed, Aug 11, 2021, 7:02 PM EDT Project Member

Cc: mho...@microsoft.com

Comment 6 by ericwilligers@chromium.org on Wed, Aug 11, 2021, 7:13 PM EDT Project Member

Cc: abalq...@microsoft.com

Comment 7 by mho...@microsoft.com on Wed, Aug 11, 2021, 8:42 PM EDT Project Member

At least the current implementation of the Windows Share dialog attempts to render itself entirely within the render space of the corresponding hwnd. It sounds a little heavy of a solution, but could we create an hwnd solely for the Share operation to control the dialog's placement?

Comment 8 by sheriffbot on Thu, Aug 12, 2021, 1:23 PM EDT Project Member

Labels: -Pri-1 Pri-2

Setting Pri-2 to match security severity Low. 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 9 by ericwilligers@chromium.org on Fri, Aug 13, 2021, 6:19 PM EDT Project Member

Cc: c...@chromium.org

Comment 10 by sheriffbot on Mon, Aug 16, 2021, 1:12 PM EDT Project Member

Labels: -Security_Impact-Stable Security_Impact-Extended

Comment 11 by alesa...@alesandroortiz.com on Tue, Sep 21, 2021, 7:27 PM EDT

ericwilligers@, mho...@, and team: Friendly ping. Any updates on this issue? No crbug activity since a month ago.

Comment 12 by ericwilligers@chromium.org on Tue, Sep 21, 2021, 7:36 PM EDT Project Member

Owner: c...@chromium.org

Reassigning to Desktop PWAs team. (I'm in the ChromeOS team.)

Comment 13 by Git Watcher on Thu, Nov 4, 2021, 5:13 PM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/c829098b81e868baa40a8fe7d113fc17b37ee2d2

commit c829098b81e868baa40a8fe7d113fc17b37ee2d2
Author: Hoch Hochkeppel <mhochk@microsoft.com>
Date: Thu Nov 04 21:12:30 2021

Accessible HWND for Windows navigator.Share

Updating the Windows implementation of navigator.Share to try to use
the HWND designated for accessibility with the WebContents. This allows
the resulting system dialog to better position/associate itself with
the WebContents, rather than just the entire window.

~~Fixed: 1238631~~
Change-Id: Ic5972234ce39ddef30115cc8139959e2146fdc3a
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3262558
Reviewed-by: Daniel Murphy <dmurph@chromium.org>
Commit-Queue: Hoch Hochkeppel <mhochk@microsoft.com>
Cr-Commit-Position: refs/heads/main@{#938502}

[modify]
https://crrev.com/c829098b81e868baa40a8fe7d113fc17b37ee2d2/chrome/browser/webshare/win/share_operation.cc

Comment 14 by sheriffbot on Fri, Nov 5, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 15 by sheriffbot on Fri, Nov 5, 2021, 1:41 PM EDT Project Member

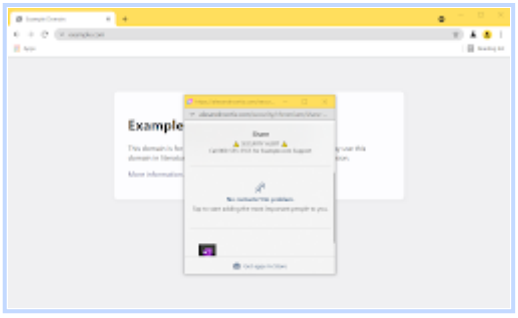
Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 16 by alesa...@alesandroortiz.com on Thu, Nov 11, 2021, 7:10 PM EST

Thanks for fix!

Verified as fixed in 98.0.4700.0 Canary on Windows 10 Version 20H2 (Build 19042.1288). Share dialog is shown below address bar as expected (see attached screenshot).

crbug-1238631-fixed.png
171 KB View Download



Comment 17 by c...@chromium.org on Thu, Nov 11, 2021, 8:30 PM EST Project Member

Owner: mho...@microsoft.com

Comment 18 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:32 PM EST Project Member

Labels: Release-0-M97

Comment 19 by amyressler@google.com on Tue, Jan 4, 2022, 1:35 PM EST Project Member

Labels: CVE-2022-0118 CVE_description-missing

Comment 20 by sheriffbot on Sat, Feb 12, 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 21 by amyressler@google.com on Thu, Mar 10, 2022, 10:40 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 22 by amyressler@chromium.org on Fri, Mar 11, 2022, 12:01 AM EST Project Member

Congratulations, Alesandro, on another one! We appreciate your efforts in reporting this issue. Given that this spoof is very overt and is a little tricky to execute in terms of tricking the user, we are extended a reduced reward in comparison to your other reports. We greatly appreciate your efforts as well as reporting these issues to us!

Comment 23 by alesa...@alesandroortiz.com on Fri, Mar 11, 2022, 12:07 AM EST

Thanks for the reward!

Comment 24 by amyressler@google.com on Fri, Mar 11, 2022, 3:04 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 25 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted