Starred by 3 users

Owner:	knollr@chromium.org **Not actively on Chrome anymore**
CC:	mkwst@chromium.org clamy@chromium.org rhalavati@chromium.org jdeblasio@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser
Modified:	Nov 2, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	2
Type:	Bug-Security

Reward-1000
Security_Severity-Low
Security_Impact-Stable
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
external_security_report
FoundIn-91
Release-0-M94
CVE-2021-37971

Issue 1219354: URL spoofing using tel:

Reported by rayya...@gmail.com on Sun, Jun 13, 2021, 6:36 PM EDT

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.101 Safari/537.36

Steps to reproduce the problem:
Similar to ~~issue 1095596~~

1. Open the apple.html
2. Right click on the link and open it in incognito mode

What is the expected behavior?
the destination of file does appear in normal mode but doesn't appear in incognito mode.

What went wrong?
described above.

Did this work before? N/A

Chrome version: 91.0.4472.101 Channel: stable
OS Version: 10.0

In the video, I've shown that in incognito mode the box doesn't show the destination of the file, but it shows in normal mode and guest mode.

apple.html
197 bytes View Download

poc.mp4
825 KB View Download

Comment 1 by sheriffbot on Sun, Jun 13, 2021, 6:37 PM EDT

Labels: external_security_report

Comment 2 by mpdenton@chromium.org on Mon, Jun 14, 2021, 7:25 PM EDT

Status: Assigned (was: Unconfirmed)
Owner: knollr@chromium.org
Labels: FoundIn-91 Security_Severity-Low
Components: UI>Browser

knollr@ PTAL? Is this related to your change from ~~issue 754394~~ or ~~issue 1095596~~?

Comment 3 by sheriffbot on Mon, Jun 14, 2021, 7:27 PM EDT

Labels: Security_Impact-Stable

Comment 4 by knollr@chromium.org on Thu, Jun 24, 2021, 10:56 AM EDT

Status: Started (was: Assigned)

Thanks for the report!
So the scenario here would be if e.g. evil.com is embedded in an iframe of legit.com and the user right clicks a link to en external protocol in the iframe and selects "Open Link in Incognito Window"? In that case we don't tell the user that this came from evil.com and they might thing it's from legit.com (even though the new window has no content from legit.com).

I think this is caused by us not setting the initiating origin when using this context menu [1] as we don't seem to want to send the referrer header to OTR windows.
A fix would be to just set the initiating origin regardless of OTR or not, uploaded a CL: crrev.com/c/2983301

[1]:
https://source.chromium.org/chromium/chromium/src/+/main:chrome/browser/renderer_context_menu/render_view_context_menu.cc;l=2303;drc=a5184a57a5dd8c32d219a5df2e28f01faf3a03de

Comment 5 by knollr@chromium.org on Tue, Jun 29, 2021, 7:11 AM EDT

Cc: rhalavati@chromium.org mkwst@chromium.org clamy@chromium.org jdeblasio@chromium.org

+some folks for visibility on the bug

Comment 6 by Git Watcher on Tue, Jul 20, 2021, 8:17 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2f311f6b6df602d7e92d992293387ee55bc7cfeb

commit 2f311f6b6df602d7e92d992293387ee55bc7cfeb
Author: Richard Knoll <knollr@chromium.org>
Date: Wed Jul 21 00:16:13 2021

Always populate the initiator origin

We show the initiator origin to the user in some browser UIs like
external protocol dialogs. This is meant to make spoofing harder as the
user would see the malicious origin where the external protocol link
came from. This also needs to be done when opening links into a new
Incognito window. We do need to make sure not to set the referrer header
for those requests though.

~~Bug: 1210354~~
Change-Id: Id00c6a6f9ba8e34433a8c042e3f7c2b7b2fca271
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2983301
Reviewed-by: Ramin Halavati <rhalavati@chromium.org>
Reviewed-by: Avi Drissman <avi@chromium.org>
Commit-Queue: Richard Knoll <knollr@chromium.org>
Cr-Commit-Position: refs/heads/master@{#903713}

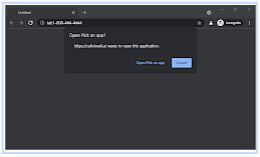
[modify] https://crrev.com/2f311f6b6df602d7e92d992293387ee55bc7cfeb/chrome/browser/renderer_context_menu/render_view_context_menu.cc
[modify] https://crrev.com/2f311f6b6df602d7e92d992293387ee55bc7cfeb/components/renderer_context_menu/render_view_context_menu_base.cc

Comment 7 by knollr@chromium.org on Mon, Jul 26, 2021, 5:16 AM EDT

Status: Fixed (was: Started)

Fixed in 94.0.4583.0, we're now showing the initiator origin when a user ends up on an external protocol using "Open Link in Incognito Window", see attached screenshot.

incognito.png
13.6 KB View Download



Comment 8 Deleted

Comment 9 by sheriffbot on Mon, Jul 26, 2021, 9:06 AM EDT

Labels: reward-topanel

Comment 10 by sheriffbot on Mon, Jul 26, 2021, 9:10 AM EDT

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

Comment 11 by amyressler@google.com on Wed, Aug 11, 2021, 2:25 PM EDT

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 12 by amyressler@chromium.org on Wed, Aug 11, 2021, 3:26 PM EDT

Congratulations, the VRP Panel has decided to award you $1,000 for this report. Thank you for reporting this issue!

Comment 13 by rayya...@gmail.com on Wed, Aug 11, 2021, 6:07 PM EDT

Request to VRP Panel: Can you please recheck this bug as this bug is similar (or reproduces) ~~Issue 1095596~~ - So the reward should match, right?

Comment 14 by amyressler@chromium.org on Wed, Aug 11, 2021, 6:22 PM EDT

Please note that there is another related bug tagged in the same comment above that garnered only a $1000 reward. Regardless, the reward decisions made by the VRP Panel are not just based on security bug type and impact, but the report quality and other factors. The VRP Panel discussed this today and determined this reward amount is commensurate for this report. I am happy to bring it back to the panel for reconsideration, but please know we did have this discussion about this report already. Thank you!

Comment 15 by amyressler@google.com on Fri, Aug 13, 2021, 11:47 AM EDT

Labels: -reward-unpaid reward-inprocess

Comment 16 by amyressler@chromium.org on Wed, Aug 18, 2021, 7:34 PM EDT

hello, rayyanh@, the VRP Panel declines to adjust the reward amount as the original reward amount has been deemed as adequate for this report.
It was also recommended that you review the Chromium Community Code of Conduct (https://chromium.googlesource.com/chromium/src/+/refs/heads/main/CODE_OF_CONDUCT.md) as some of your comments to the security team and developers in bug reports and emails over time are potentially violating this code of conduct.

We greatly appreciate your bug reports, but please remember to be respectful and kind to the community members with whom you interact in the course of discussing security issues. Thank you!

Comment 17 by rayya...@gmail.com on Wed, Aug 18, 2021, 7:47 PM EDT

"as some of your comments to the security team and developers in bug reports and emails over time are potentially violating this code of conduct. "

I'm so sorry If some of my comments were potentially violating the code of conduct, please note that It was never my intention to hurt someone. I'll be careful next time.

Comment 18 by amyressler@chromium.org on Mon, Sep 20, 2021, 6:23 PM EDT

Labels: Release-0-M94

Comment 19 by amyressler@google.com on Tue, Sep 21, 2021, 1:19 PM EDT

Labels: CVE-2021-37971 CVE_description-missing

Comment 20 by amyressler@google.com on Fri, Oct 8, 2021, 5:31 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 21 by sheriffbot on Tue, Nov 2, 2021, 1:30 PM EDT

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