☆ Starred by 2 users

Owner:	ydago@chromium.org
CC:	pastarmovj@chromium.org ydago@chromium.org aee@chromium.org zmin@chromium.org georgesak@chromium.org tiborg@chromium.org poromov@chromium.org
Status:	Fixed *(Closed)*
Components:	Enterprise
Modified:	Jun 13, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Windows, Mac
Pri:	1
Type:	Bug-Security

reward-500
Security_Impact-Stable
Security_Severity-Medium
Arch-x86_64
allpublic
reward-inprocess
Via-Wizard-Security
CVE_description-submitted
M-82
Release-0-M83
CVE-2020-6480

Issue 1054966: Policy page opens a file dialogue even if the AllowFileSelectionDialogs policy is set to false

Reported by nurma...@protonmail.com on Fri, Feb 21, 2020, 5:14 PM EST

Code

UserAgent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0

Steps to reproduce the problem:
1. Start the Chromium browser with the "AllowFileSelectionDialogue" policy disabled.
2. Open the internal policy page (chrome://policy).
3. Press the "Export to JSON" button.

What is the expected behavior?
The button shouldn't open a file selection dialog.

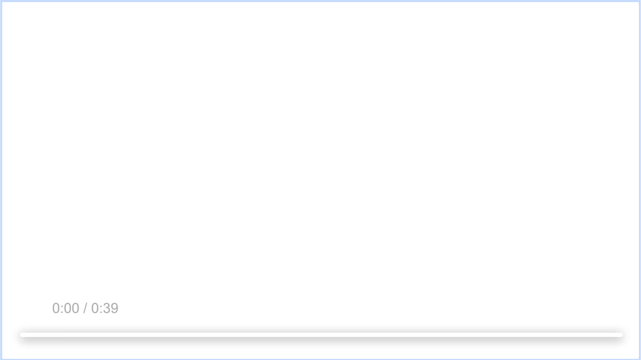
What went wrong?
The button opens a file dialog.

Did this work before? N/A

Chrome version: 82.0.4062.3 (Official Build) dev (64-bit) (cohort: Dev) Channel: stable
OS Version: 10.0
Flash Version: 32.0.0.330

This is a rather critical bug, as opening the file selection dialog usually allows access to the systems file explorer and therefore full access to execute files on the system.
This could compromise machines in public that users are only meant to be able to use chrome in; online browser VMs like caracal.club or Cryb; and other such systems.

0004992.mp4
1.6 MB View Download



Comment 1 by nurma...@protonmail.com on Fri, Feb 21, 2020, 5:29 PM EST

Please also note that I tested this in both the developer version (82.0.4062.3 (Official Build) dev (64-bit) (cohort: Dev)) as well as the stable version (80.0.3987.116 (Official Build) (64-bit) (cohort: Stable Installs Only)) of Google Chrome and it worked in both.
I used Firefox to post this bug report, which is why the User Agent that was automatically included in the report is wrong.
The User Agent of the Chrome Browser in test was "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36".

Comment 2 by ajgo@google.com on Fri, Feb 21, 2020, 7:16 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: ydago@chromium.org
Cc: zmin@chromium.org poromov@chromium.org
Labels: Security_Impact-Stable Security_Severity-Medium
Components: Enterprise

Thanks for the report.

I have confirmed that this is happening on chrome://policy and that no other chrome:// pages have this bug.

Assigning to ydago via "blame" from https://source.chromium.org/chromium/chromium/src/+/master:components/policy/resources/webui/policy.html.

Comment 3 by sheriffbot on Sat, Feb 22, 2020, 1:08 PM EST Project Member

Labels: Target-81 M-81

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 4 by sheriffbot on Sat, Feb 22, 2020, 1:44 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 5 by poromov@chromium.org on Sat, Feb 22, 2020, 6:35 PM EST Project Member

Cc: georgesak@chromium.org
Labels: OS-Linux OS-Mac

According to this comment it's WAI: https://cs.chromium.org/chromium/src/chrome/browser/ui/webui/policy_ui_handler.cc?l=1017&rcl=8d1fe43a8abd9cf0c2d6beb1fb7a19ab16c0401e
The code (and comment) was added in 2017: https://crrev.com/c/579568/ Feature bug is ~~https://crbug.com/745880~~
urusant@ is not on the team anymore, so adding Georges.

Comment 6 by nurma...@protonmail.com on Sat, Feb 22, 2020, 7:28 PM EST

Allowing the user to open a file selection dialog allows an user to delete, create, edit and run files on the system as they wish, and could compromise systems that users are only allowed to use Chrome/Chromium on.
There is no good reason why this should be allowed on the 'Export to JSON' button on the policy screen. Most reasons one may have to disable the file explorer dialog would also apply to this dialog.
This is dangerous, especially as it is not even warned about in the documentation of the AllowFileSelectionDialogs policy ('whenever the user performs an action which would provoke a file selection dialog [...] a message is displayed instead and the user is assumed to have clicked Cancel')

Comment 7 by poromov@chromium.org on Mon, Feb 24, 2020, 2:27 PM EST Project Member

Cc: pastarmovj@chromium.org

I agree that this may lead to unwanted behavior according to your description, however as not an expert on desktop platform I can't weigh how well it aligns with our guarantees for the policy on Windows, Linux, Mac. I refer to Chrome Enterprise Browser team to answer it.
However, if we'll want to fix it, we need to check other places where file dialog might be created as the code is not resilient to skipping policy checks :-(

Comment 8 by pastarmovj@chromium.org on Tue, Feb 25, 2020, 11:41 AM EST Project Member

Status: Untriaged (was: Assigned)
Owner: ----
Cc: ydago@chromium.org

I am unassigning from Yann so that we can go over this bug in the prioritization session on Thursday and evaluate the priority.

Comment 9 by georgesak@chromium.org on Wed, Feb 26, 2020, 1:55 PM EST Project Member

#6 makes a good point.

I have no objections to changing this behavior and honoring the policy.

Comment 10 by kenrb@chromium.org on Fri, Feb 28, 2020, 3:57 PM EST Project Member

parstarmovj@: Was this looked at for triage on your side yesterday? It's flagged as a medium severity security bug so it should have an owner.

Comment 11 by pastarmovj@chromium.org on Tue, Mar 3, 2020, 8:12 AM EST Project Member

Owner: ydago@chromium.org
Labels: -M-81 -Target-81 M-82

Reassigning back to Yann then

Please consider disabling the export button when the policy is effective.

Yann, please consider this as a P1 (likely higher than most other things on the list so please prioritize accordingly).

As a side note - offering a copy JSON to clipboard might be beneficial in the presence of this policy. Filed this here https://bugs.chromium.org/p/chromium/issues/detail?id=1058001

Comment 12 by ydago@chromium.org on Tue, Mar 3, 2020, 1:33 PM EST Project Member

Status: Started (was: Untriaged)

Comment 13 by bugdroid on Fri, Mar 6, 2020, 3:02 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/3ab7de11a8c950ad4a094a0092db50db8c7c25bd

commit 3ab7de11a8c950ad4a094a0092db50db8c7c25bd
Author: Yann Dago <ydago@chromium.org>
Date: Fri Mar 06 20:01:31 2020

Policy WebUI: Enforce AllowFileSelectionDialogs policy on export json

~~Bug: 1054066~~

Change-Id: I93f73023e6e6bdc24c329c36b2b14323522a078c
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2085156
Commit-Queue: Yann Dago <ydago@chromium.org>
Auto-Submit: Yann Dago <ydago@chromium.org>
Reviewed-by: Julian Pastarmov <pastarmovj@chromium.org>
Cr-Commit-Position: refs/heads/master@{#747820}

[modify] https://crrev.com/3ab7de11a8c950ad4a094a0092db50db8c7c25bd/chrome/browser/ui/webui/policy_ui_browsertest.cc
[modify] https://crrev.com/3ab7de11a8c950ad4a094a0092db50db8c7c25bd/chrome/browser/ui/webui/policy_ui_handler.cc

Comment 14 by ydago@chromium.org on Fri, Mar 6, 2020, 3:25 PM EST Project Member

Status: Fixed (was: Started)

Comment 15 by sheriffbot on Sat, Mar 7, 2020, 2:02 PM EST Project Member

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

Comment 16 by natashapabrai@google.com on Mon, Mar 9, 2020, 3:22 PM EDT Project Member

Labels: reward-topanel

Comment 17 by natashapabrai@google.com on Wed, Mar 11, 2020, 6:33 PM EDT Project Member

Labels: -reward-topanel reward-unpaid reward-500

*** 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 18 by natashapabrai@google.com on Wed, Mar 11, 2020, 6:37 PM EDT Project Member

Congrats! The Panel decided to award $500 for this report!

Comment 19 by natashapabrai@google.com on Wed, Mar 11, 2020, 6:45 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 20 by ajgo@chromium.org on Thu, Apr 16, 2020, 11:57 AM EDT Project Member

Cc: aee@chromium.org tiborg@chromium.org

CC aee@ & tiborg for visibility.

Comment 21 by adetaylor@google.com on Wed, May 13, 2020, 12:28 PM EDT Project Member

nurmarvin@protonmail.com - thanks for the report; how would you like to be credited in the Chrome release notes?

Comment 22 by nurma...@protonmail.com on Wed, May 13, 2020, 12:31 PM EDT

I think I'll just go with my full name, which would be "Marvin Witt".

Comment 23 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 24 by adetaylor@google.com on Fri, May 15, 2020, 4:26 PM EDT Project Member

Thanks!

Comment 25 by adetaylor@chromium.org on Mon, May 18, 2020, 11:58 AM EDT Project Member

Labels: CVE-2020-6480 CVE_description-missing

Comment 26 by adetaylor@chromium.org on Wed, May 20, 2020, 11:44 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 27 by sheriffbot on Sat, Jun 13, 2020, 2:59 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