Starred by 2 users

Owner:	qin...@chromium.org
CC:	qin...@chromium.org xingliu@chromium.org dtrainor@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Downloads
Modified:	Sep 23, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	2
Type:	Bug-Security

reward-500
Security_Severity-Low
Security_Impact-Stable
allpublic
reward-inprocess
CVE_description-submitted
Release-0-M83
CVE-2020-6488

Issue 1044277: Security: Possible to bypass restrictions on multiple downloads by initiating download from data: frame

Reported by derce...@gmail.com on Tue, Jan 21, 2020, 3:02 PM EST

Code

VULNERABILITY DETAILS
Typically it's not possible for a page to download more than one file without further user interaction. However, by initiating a download from an opaque origin, a page can, in certain circumstances, download multiple files.

VERSION
Chrome Version: Tested on 79.0.3945.130 (stable) and 81.0.4034.0 (canary)
Operating System: Windows 10, version 1909

REPRODUCTION CASE
1. Open index.html.
2. This page will initiate a download of an empty text file, one download every 5 seconds.

Some explanation of that's happening:

If on a page you have a data: sub-frame that performs the following steps:

```
var newWindow = open();
newWindow.location.href = "...url-to-download-file...";
```

The frame will be able to download multiple files without any restrictions.

From some testing, this won't work if the frame tries to download multiple files by setting its own location, or that of its parent. It also won't work if the new window the frame opens points to a regular http/https page (it has to be something like about:blank).

However, going through the above steps would likely mean that the user would have to interact with the page first (e.g. by clicking it), so that the page could successfully call window.open.

In the demonstration, there's no user interaction required, because the page changes its visible URL to about:blank (there are some comments in main.js that explain this). A data: frame on the page will then be able to download multiple files without any restrictions.

CREDIT INFORMATION
Reporter credit: David Erceg

index.html
203 bytes View Download

main.js
1.0 KB View Download

Comment 1 by est...@chromium.org on Tue, Jan 21, 2020, 5:40 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: dtrainor@chromium.org
Cc: xingliu@chromium.org qin...@chromium.org
Components: UI>Browser>Downloads

Downloads folks, could you please take a look and see if this is working as intended or not? Thanks!

Comment 2 by est...@chromium.org on Wed, Jan 22, 2020, 10:59 AM EST Project Member

Labels: Security_Impact-Stable Security_Severity-Low OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows

Tentatively triaging as Low severity, though I'm not sure this should be tracked as a security bug, and would still like to hear from downloads people on whether this is a known issue or not.

Comment 3 by sheriffbot@chromium.org on Wed, Jan 22, 2020, 12:12 PM EST Project Member

Labels: 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 4 by dtrainor@chromium.org on Thu, Jan 23, 2020, 12:38 AM EST Project Member

Owner: qin...@chromium.org
Cc: dtrainor@chromium.org

Min can you take a look? Thanks!

Comment 5 by bugdroid on Tue, Feb 11, 2020, 2:02 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src.git/+/220ecb7e354511f3c457d99841a9c09ac3964995

commit 220ecb7e354511f3c457d99841a9c09ac3964995
Author: Min Qin <qinmin@chromium.org>
Date: Tue Feb 11 18:59:47 2020

Fix an issue that opaque origin triggered download is not throttled

If a download is triggered by opaque origin, currently we create an origin
from main WebContents' URL to determine if the download should be blocked.
However, if main WebContents' URL is also an opaque origin, the newly
created origin will be different from the previous origin. And making
the download always allowed.
This CL fixes the issue by using the originating opaque origin instead
if the WebContents' origin is opaque. An alternative solution is to
assign a dedicated opaque origin to the main WebContents.

~~BUG=1044277~~

Change-Id: Ia38280f4237ba5cd35c7afcf350734833fb9d002
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2048843
Commit-Queue: Min Qin <qinmin@chromium.org>
Reviewed-by: Xing Liu <xingliu@chromium.org>
Cr-Commit-Position: refs/heads/master@{#740375}

[modify] https://crrev.com/220ecb7e354511f3c457d99841a9c09ac3964995/chrome/browser/download/download_request_limiter.cc
[modify] https://crrev.com/220ecb7e354511f3c457d99841a9c09ac3964995/chrome/browser/download/download_request_limiter_unittest.cc

Comment 6 by qin...@chromium.org on Tue, Feb 11, 2020, 3:55 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 7 by sheriffbot on Fri, Feb 14, 2020, 7:50 PM EST Project Member

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

Comment 8 by natashapabrai@google.com on Tue, Feb 18, 2020, 11:14 AM EST Project Member

Labels: reward-topanel

Comment 9 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:00 PM EST 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 10 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:05 PM EST Project Member

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

Comment 11 by natashapabrai@google.com on Wed, Feb 19, 2020, 7:09 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 12 by adetaylor@google.com on Fri, May 15, 2020, 3:55 PM EDT Project Member

Labels: Release-0-M83

Comment 13 by adetaylor@chromium.org on Mon, May 18, 2020, 11:59 AM EDT Project Member

Labels: CVE-2020-6488 CVE_description-missing

Comment 14 by sheriffbot on Wed, May 20, 2020, 3:01 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 15 by adetaylor@chromium.org on Wed, May 20, 2020, 11:44 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 16 by qin...@chromium.org on Thu, Sep 23, 2021, 8:03 PM EDT Project Member

~~Issue 1055073~~ has been merged into this issue.