☆ Starred by 3 users

Owner:	drubery@chromium.org
CC:	drubery@chromium.org vakh@chromium.org rsleevi@chromium.org nmehta@google.com
Status:	Fixed *(Closed)*
Components:	Services>Safebrowsing UI>Browser>Downloads
Modified:	Jul 29, 2022
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-12-01
OS:	Mac
Pri:	2
Type:	Bug-Security

SafeBrowsing-Triaged
reward-500
Security_Severity-Low
allpublic
reward-inprocess
CVE_description-submitted
external_security_report
FoundIn-93
Security_Impact-Extended
Release-0-M102
CVE-2022-1874

BlockedOn:	Issue 1241961

View details

Issue 1251588: Security: download protection bypass on macOS with .inetloc

Reported by houji...@gmail.com on Tue, Sep 21, 2021, 8:12 AM EDT

Code

VERSION
Chrome Version: Version 93.0.4577.82 (Official Build) (arm64)
Operating System: macOS Big Sur, 11.5.2

REPRODUCTION CASE
Vladimir Metnew reported that .fileloc files on macOS can bypass download protection in 2019:https://bugs.chromium.org/p/chromium/issues/detail?id=1029375
However, .inetloc files are similar to .fileloc files and .inetloc is not in blacklist.
When download a .fileloc file in chrome, chrome will warn:"This type of file can harm your computer.Do you want to keep test.fileloc anyway?"
But when download a .inetloc file in chrome there is no warning and if victim double click the .inetloc file they download then attacker may execute arbitrary commands.
I provided a test.inetloc which can open calc for test.

test.inetloc
295 bytes Download

Comment 1 by sheriffbot on Tue, Sep 21, 2021, 8:16 AM EDT Project Member

Labels: external_security_report

Comment 2 by ajgo@google.com on Tue, Sep 21, 2021, 2:08 PM EDT Project Member

Owner: drubery@chromium.org
Cc: vakh@chromium.org
Labels: FoundIn-93 OS-Mac
Components: Services>Safebrowsing UI>Browser>Downloads

drubery - it feels like this should be added to the list of dangerous file types for Mac.

Comment 3 by ajgo@google.com on Tue, Sep 21, 2021, 2:09 PM EDT Project Member

Labels: Security_Severity-Low

Comment 4 by sheriffbot on Tue, Sep 21, 2021, 2:13 PM EDT Project Member

Labels: Security_Impact-Extended

Comment 5 by sheriffbot on Tue, Sep 21, 2021, 2:23 PM EDT Project Member

Status: Assigned (was: Unconfirmed)

Comment 6 by sheriffbot on Wed, Sep 22, 2021, 1:28 PM EDT Project Member

Labels: -Pri-3 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 7 by vakh@chromium.org on Fri, Sep 24, 2021, 3:01 PM EDT Project Member

Labels: SafeBrowsing-Triaged

Comment 8 by drubery@chromium.org on Fri, Sep 24, 2021, 4:34 PM EDT Project Member

Blockedon: 1241961
NextAction: 2021-10-19

I agree that this is just a matter of changing the file type policy. We're currently running an experiment with that policy, so I'd prefer not to fix this until that experiment wraps up with M95 Stable.

The risk here is pretty low, as we do contact Safe Browsing for these downloads. We just don't show a warning every time.

Comment 9 by drubery@chromium.org on Mon, Oct 4, 2021, 8:15 PM EDT Project Member

Cc: rsleevi@chromium.org drubery@chromium.org

~~Issue 1255337~~ has been merged into this issue.

Comment 10 by monor...@bugs.chromium.org on Tue, Oct 19, 2021, 8:00 AM EDT

The NextAction date has arrived: 2021-10-19

Comment 11 by drubery@chromium.org on Thu, Oct 28, 2021, 1:58 PM EDT Project Member

NextAction: 2021-12-01

The experiment is still ongoing, so continuing to push this.

Comment 12 by houji...@gmail.com on Thu, Nov 25, 2021, 10:47 PM EST

Same problem exists in firefox and the mozilla security advisory is here:
https://www.mozilla.org/en-US/security/advisories/mfsa2021-48/#CVE-2021-38510

Comment 13 by monor...@bugs.chromium.org on Wed, Dec 1, 2021, 7:00 AM EST

The NextAction date has arrived: 2021-12-01

Comment 14 by houji...@gmail.com on Tue, Dec 28, 2021, 10:36 PM EST

Hello, anyone here???

Comment 15 by Git Watcher on Thu, Mar 24, 2022, 6:43 PM EDT Project Member

Status: Fixed (was: Assigned)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/784abfd18c9b7e733ec6031ab02912f2ebd27aeb

commit 784abfd18c9b7e733ec6031ab02912f2ebd27aeb
Author: Daniel Rubery <drubery@chromium.org>
Date: Thu Mar 24 22:42:54 2022

Add inetloc to download_file_types.asciipb

This file type is comparable to webloc, so treat it the same way.

~~Fixed: 1251588~~
Change-Id: I311fa69bcf155eb2882ebb5706404a134f9fd857
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3549458
Auto-Submit: Daniel Rubery <drubery@chromium.org>
Reviewed-by: Xinghui Lu <xinghuilu@chromium.org>
Commit-Queue: Xinghui Lu <xinghuilu@chromium.org>
Cr-Commit-Position: refs/heads/main@{#985052}

[modify]
https://crrev.com/784abfd18c9b7e733ec6031ab02912f2ebd27aeb/components/safe_browsing/content/resources/download_file_types.asciipb
[modify]
https://crrev.com/784abfd18c9b7e733ec6031ab02912f2ebd27aeb/components/safe_browsing/content/resources/download_file_types_experiment.asciipb
[modify] https://crrev.com/784abfd18c9b7e733ec6031ab02912f2ebd27aeb/tools/metrics/histograms/enums.xml

Comment 16 by sheriffbot on Sun, Mar 27, 2022, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 17 by sheriffbot on Sun, Mar 27, 2022, 1:41 PM EDT Project Member

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

Comment 18 by amyressler@google.com on Thu, Mar 31, 2022, 5:15 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 19 by amyressler@chromium.org on Thu, Mar 31, 2022, 5:53 PM EDT Project Member

Hello, thank you for reporting this issue to us. The Chrome VRP would like to extend a $500 thank you for this report. A member of our finance team will be in touch to arrange payment. Thank you for your efforts and reporting this issue to us!

Comment 20 by amyressler@google.com on Fri, Apr 1, 2022, 4:16 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 21 by amyressler@chromium.org on Mon, May 23, 2022, 10:04 PM EDT Project Member

Labels: Release-0-M102

Comment 22 by amyressler@chromium.org on Mon, May 23, 2022, 10:20 PM EDT Project Member

Hello OP, what is the name/handle/tag you would like us to use in acknowledging you for this issue?

Comment 23 by houji...@gmail.com on Tue, May 24, 2022, 9:16 AM EDT

Please use "hjy79425575". Thank you!

Comment 24 by amyressler@google.com on Tue, May 24, 2022, 2:17 PM EDT Project Member

Labels: CVE-2022-1874 CVE_description-missing

Comment 25 by sheriffbot on Fri, Jul 1, 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 26 by amyressler@chromium.org on Thu, Jul 21, 2022, 2:45 PM EDT Project Member

Cc: nmehta@google.com

Comment 27 by amyressler@google.com on Wed, Jul 27, 2022, 5:26 PM EDT Project Member

Labels: CVE_description-submitted -CVE_description-missing

Comment 28 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:26 PM EDT Project Member

Labels: -CVE_description-missing --CVE_description-missing