Starred by 4 users

Owner:	qin...@chromium.org
CC:	qin...@chromium.org qinmin@google.com dtrainor@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>DataTransfer UI>Browser>Downloads
Modified:	May 12, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Windows
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
Target-88
M-88
LTS-Security-86
LTS-Security-NotApplicable-86
merge-merged-4324
merge-merged-88
external_security_report
merge-merged-4389
merge-merged-89
Release-3-M88
CVE-2021-21150

Issue 1172192: Security: UAF in Drag and Drop Download

Reported by rapid...@gmail.com on Fri, Jan 29, 2021, 6:01 AM EST

Code

VULNERABILITY DETAILS
in Window, the chrome can "drag and drop download" [0]
it is asynchronously executed on UI thread [1][2]. the DragDownloadFile object have raw DragDownloadFileUI pointer.
it is safe because DragDownloadFileUI is deleted on UI thread using PostTask[3].
but DragDownloadFileUI have raw WebContents pointer.[4]. it can be freed before executing "drag and drop download"[2].
and WebContents pointer is used on it [5]. so can trigger UAF

[0] :
https://source.chromium.org/chromium/chromium/src/+/master:content/browser/web_contents/web_contents_view_aura.cc;drc=6cdb24a4ce9d4151035c1f133833137d2e2881d1;l=244
[1] :
https://source.chromium.org/chromium/chromium/src/+/master:ui/base/dragdrop/os_exchange_data_provider_win.cc;drc=6f2046bedac15dc31e1cdf9a5e4a5eadd46231ae;l=928
[2] :
https://source.chromium.org/chromium/chromium/src/+/master:content/browser/download/drag_download_file.cc;drc=6cdb24a4ce9d4151035c1f133833137d2e2881d1;l=216
[3] :
https://source.chromium.org/chromium/chromium/src/+/master:content/browser/download/drag_download_file.cc;drc=6cdb24a4ce9d4151035c1f133833137d2e2881d1;l=199
[4] :
https://source.chromium.org/chromium/chromium/src/+/master:content/browser/download/drag_download_file.cc;drc=6cdb24a4ce9d4151035c1f133833137d2e2881d1;l=168
[5] :
https://source.chromium.org/chromium/chromium/src/+/master:content/browser/download/drag_download_file.cc;drc=6cdb24a4ce9d4151035c1f133833137d2e2881d1;l=82
VERSION
Chrome Version: latest chrome
Operating System: only Window

REPRODUCTION CASE

apply patch.diff to simulate a compromised renderer
navigate index.html and touch page

once touch the page, your cursor is changed to drag the cursor.
and drop to the desktop using right-click.(slowly click to move/copy here) it will be crashed

plz see video

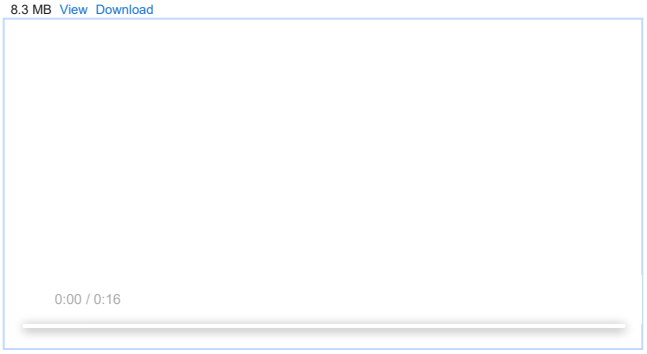
CREDIT INFORMATION

Reporter credit: Woojin Oh of STEALIEN(@pwn_exploit)

patch.txt
18.9 KB View Download

bandicam 2021-01-29 19-56-47-218.mp4

8.3 MB View Download



index.html
91 bytes View Download

Comment 1 by sheriffbot on Fri, Jan 29, 2021, 6:03 AM EST Project Member

Labels: external_security_report

Comment 2 by rsleevi@chromium.org on Fri, Jan 29, 2021, 3:55 PM EST Project Member

Cc: dtrainor@chromium.org qin...@chromium.org
Labels: Security_Severity-High
Components: UI>Browser>Downloads Blink>DataTransfer

Thanks for the report and detailed analysis! Adding some labels while I work to reproduce. CC'ing a few folks though, since you're right that a raw WebContents* does raise some eyebrows.

Comment 3 by qin...@chromium.org on Fri, Jan 29, 2021, 4:47 PM EST Project Member

Thanks for reporting this. Looks like the easiest fix is to pass a RenderViewHost Id to DragDownloadFileUI, and use it to retrieve the WebContents if needed.

Comment 4 by rsleevi@chromium.org on Fri, Jan 29, 2021, 7:21 PM EST Project Member

Status: Assigned (was: Unconfirmed)
Owner: qin...@chromium.org
Labels: OS-Windows

Comment 5 by sheriffbot on Sat, Jan 30, 2021, 1:27 PM EST Project Member

Labels: -Pri-3 Pri-1

Setting Pri-1 to match security severity High. 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 6 by rsleevi@chromium.org on Mon, Feb 1, 2021, 3:22 PM EST Project Member

Labels: Security_Impact-Stable

qinmin: I'm having some trouble with the bisect, but on source inspection, as far as I can tell, this pattern goes to at least Stable. If I've misdiagnosed, feel free to shout at me (especially if/when sheriffbot gets shouty).

Comment 7 by sheriffbot on Tue, Feb 2, 2021, 12:51 PM EST Project Member

Labels: Target-88 M-88

Setting milestone and target because of Security_Impact=Stable and high severity.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 8 by bugdroid on Tue, Feb 2, 2021, 2:09 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/99dc876a13df19f3512bcfb97e794ab5d1b28905

commit 99dc876a13df19f3512bcfb97e794ab5d1b28905
Author: Min Qin <qinmin@chromium.org>
Date: Tue Feb 02 19:06:51 2021

Stop using raw WebContents ptr in DragDownloadFile

~~BUG=1172192~~

Change-Id: Ie029713553ff88c1e271db1c84396e1ddda19286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2666189
Reviewed-by: Xing Liu <xingliu@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#849692}

[modify] https://crrev.com/99dc876a13df19f3512bcfb97e794ab5d1b28905/content/browser/download/drag_download_file_browsertest.cc
[modify] https://crrev.com/99dc876a13df19f3512bcfb97e794ab5d1b28905/content/browser/download/drag_download_file.cc

Comment 9 by qin...@chromium.org on Tue, Feb 2, 2021, 3:20 PM EST Project Member

Status: Fixed (was: Assigned)

Comment 10 by sheriffbot on Wed, Feb 3, 2021, 12:44 PM EST Project Member

Labels: reward-topanel

Comment 11 by sheriffbot on Wed, Feb 3, 2021, 1:59 PM EST Project Member

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

Comment 12 by bugdroid on Wed, Feb 3, 2021, 2:17 PM EST Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3eda2771096d422aa90adfe8297f470df797bd5e

commit 3eda2771096d422aa90adfe8297f470df797bd5e
Author: Min Qin <qinmin@chromium.org>

Date: Wed Feb 03 19:14:01 2021

Add a method to disable download from starting a foreground service if
activities are invisible

This CL adds a method in AppHooks to make us not start a new foreground
service if Chrome activities are not visible. If a foreground service is
already started, the new notification updates will still use the existing
foreground serviec to change notification Ids if necessary.

~~BUG=1172192~~

Change-Id: I9d9ee74ed3e84597850ccb935c01851968dbab10
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2667777
Reviewed-by: David Trainor <dtrainor@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Commit-Position: refs/heads/master@{#850218}

[modify]
https://crrev.com/3eda2771096d422aa90adfe8297f470df797bd5e/chrome/android/java/src/org/chromium/chrome/browser/download/DownloadForegroundServiceManager.java
[modify] https://crrev.com/3eda2771096d422aa90adfe8297f470df797bd5e/chrome/android/java/src/org/chromium/chrome/browser/AppHooks.java
[modify]
https://crrev.com/3eda2771096d422aa90adfe8297f470df797bd5e/chrome/android/java/src/org/chromium/chrome/browser/download/DownloadNotificationService.java

Comment 13 by sheriffbot on Wed, Feb 3, 2021, 2:19 PM EST Project Member

Labels: Merge-Request-89 Merge-Request-88

Requesting merge to stable M88 because latest trunk commit (850218) appears to be after stable branch point (827102).

Requesting merge to beta M89 because latest trunk commit (850218) appears to be after beta branch point (843830).

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 14 by qin...@chromium.org on Wed, Feb 3, 2021, 2:25 PM EST Project Member

The 2nd CL has a wrong bug number, should be only the first CL.

Comment 15 by sheriffbot on Thu, Feb 4, 2021, 2:21 PM EST Project Member

Labels: -Merge-Request-89 Merge-Review-89 Hotlist-Merge-Review

This bug requires manual review: M89's targeted beta branch promotion date has already passed, so this requires manual review
Before a merge request will be considered, the following information is required to be added to this bug:

1. Does your merge fit within the Merge Decision Guidelines?
- Chrome: https://chromium.googlesource.com/chromium/src.git/+/master/docs/process/merge_request.md#when-to-request-a-merge
- Chrome OS: https://goto.google.com/cros-release-branch-merge-guidelines
2. Links to the CLs you are requesting to merge.
3. Has the change landed and been verified on ToT?
4. Does this change need to be merged into other active release branches (M-1, M+1)?
5. Why are these changes required in this milestone after branch?
6. Is this a new feature?
7. If it is a new feature, is it behind a flag using finch?

Chrome OS Only:
8. Was the change reviewed and approved by the Eng Prod Representative? See Eng Prod ownership by component: http://go/cros-engprodcomponents

Please contact the milestone owner if you have questions.
Owners: benmason@(Android), bindusuvarna@(iOS), geohsu@(ChromeOS), pbommana@(Desktop)

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot

Comment 16 by pbommana@google.com on Mon, Feb 8, 2021, 12:30 AM EST Project Member

qinmin@ request to provide answers to questions from comment#15

Comment 17 by qin...@chromium.org on Mon, Feb 8, 2021, 12:51 AM EST Project Member

1. yes
2. https://chromium-review.googlesource.com/c/chromium/src/+/2666189
3.yes
4. Yes for M89
5. Fix a UAF security issue
6. No

Comment 18 by adetaylor@google.com on Mon, Feb 8, 2021, 7:33 PM EST Project Member

Labels: -Merge-Review-89 Merge-Approved-89

Approving merge to M89, branch 4389.

Comment 19 by bugdroid on Tue, Feb 9, 2021, 5:05 PM EST Project Member

Labels: -merge-approved-89 merge-merged-89 merge-merged-4389

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/1ebd5af895d8231ff103b672f9c9e8d60ee62d68

commit 1ebd5af895d8231ff103b672f9c9e8d60ee62d68
Author: Min Qin <qinmin@chromium.org>
Date: Tue Feb 09 22:05:21 2021

Stop using raw WebContents ptr in DragDownloadFile

~~BUG=1172192~~

(cherry picked from commit 99dc876a13df19f3512bcfb97e794ab5d1b28905)

Change-Id: Ie029713553ff88c1e271db1c84396e1ddda19286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2666189
Reviewed-by: Xing Liu <xingliu@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#849692}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2683515
Cr-Commit-Position: refs/branch-heads/4389@{#868}
Cr-Branched-From: 9251c5db2b6d5a59fe4eac7aafa5fed37c139bb7-refs/heads/master@{#843830}

[modify] https://crrev.com/1ebd5af895d8231ff103b672f9c9e8d60ee62d68/content/browser/download/drag_download_file_browsertest.cc
[modify] https://crrev.com/1ebd5af895d8231ff103b672f9c9e8d60ee62d68/content/browser/download/drag_download_file.cc

Comment 20 by amyressler@google.com on Wed, Feb 10, 2021, 1:59 PM EST Project Member

Labels: -reward-topanel reward-unpaid reward-20000

*** 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 21 by adetaylor@chromium.org on Wed, Feb 10, 2021, 4:24 PM EST Project Member

Labels: -Merge-Request-88 Merge-Approved-88

Approving merge to M88, branch 4324. Please merge by the end of Thursday PST to get into next Tuesday's release.

Comment 22 by amyressler@google.com on Wed, Feb 10, 2021, 5:55 PM EST Project Member

Congratulations, Woojin Oh! The VRP Panel has decided to award you $20,000 for this report. Excellent work and thank you for your efforts!

Comment 23 by amyressler@google.com on Thu, Feb 11, 2021, 3:59 PM EST Project Member

Labels: -reward-unpaid reward-inprocess

Comment 24 by srinivassista@google.com on Thu, Feb 11, 2021, 4:22 PM EST Project Member

Please help complete the merge before friday (Feb 12) - 12pm PST,

Comment 25 by bugdroid on Fri, Feb 12, 2021, 5:45 PM EST Project Member

Labels: -merge-approved-88 merge-merged-4324 merge-merged-88

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/3a6f6fbfd8fa87c10a255c56501446bec1ccc3dc

commit 3a6f6fbfd8fa87c10a255c56501446bec1ccc3dc
Author: Min Qin <qinmin@chromium.org>
Date: Fri Feb 12 22:45:08 2021

Stop using raw WebContents ptr in DragDownloadFile

~~BUG=1172102~~

(cherry picked from commit 99dc876a13df19f3512bcfb97e794ab5d1b28905)

Change-Id: Ie029713553ff88c1e271db1c84396e1ddda19286
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2666189
Reviewed-by: Xing Liu <xingliu@chromium.org>
Commit-Queue: Min Qin <qinmin@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#849692}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2692927
Reviewed-by: Shakti Sahu <shaktisahu@chromium.org>
Cr-Commit-Position: refs/branch-heads/4324@{#2200}
Cr-Branched-From: c73b5a651d37a6c4d0b8e3262cc4015a5579c6c8-refs/heads/master@{#827102}

[modify] https://crrev.com/3a6f6fbfd8fa87c10a255c56501446bec1ccc3dc/content/browser/download/drag_download_file_browsertest.cc
[modify] https://crrev.com/3a6f6fbfd8fa87c10a255c56501446bec1ccc3dc/content/browser/download/drag_download_file.cc

Comment 26 by adetaylor@google.com on Fri, Feb 12, 2021, 7:35 PM EST Project Member

Labels: Release-3-M88

Comment 27 by achuith@chromium.org on Thu, Feb 18, 2021, 8:40 PM EST Project Member

Labels: LTS-Security-NotApplicable-86

Comment 28 by amyressler@google.com on Mon, Feb 22, 2021, 4:31 PM EST Project Member

Labels: CVE-2021-21150 CVE_description-missing

Comment 29 by amyressler@google.com on Mon, Feb 22, 2021, 4:33 PM EST Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 30 by gov...@chromium.org on Tue, Feb 23, 2021, 4:46 PM EST Project Member

Cc: qinmin@google.com

Comment 31 by asumaneev@google.com on Thu, Apr 22, 2021, 10:50 AM EDT Project Member

Labels: LTS-Security-86

Comment 32 by sheriffbot on Wed, May 12, 2021, 1:51 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 33 by amyressler@chromium.org on Wed, May 12, 2021, 2:56 PM EDT Project Member

Hello! We consider attachments/pocs included with reports to be an integral part of the report, so I've un-deleted them. Thanks!