Starred by 3 users

Owner:	mastiz@chromium.org
CC:	carlosil@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>History
Modified:	Aug 26, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	2021-05-03
OS:	Linux, Android, Windows, Chrome, Fuchsia
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
reward-20000
CVE_description-submitted
M-90
Target-90
merge-merged-4240
LTS-Security-86
external_security_report
LTS-Merge-Approved-86
merge-merged-4430
merge-merged-90
merge-merged-4472
merge-merged-91
merge-merged-4430_101
Release-3-M90
CVE-2021-30516

Issue 1201446: Security: heap-buffer-overflow in CreateFaviconImageSkia

Reported by zhanj...@gmail.com on Wed, Apr 21, 2021, 8:41 PM EDT

Code

VULNERABILITY DETAILS

in function CreateFaviconImageSkia, the size of bitmaps can be small than original_sizes's, access bitmaps[index] may cause heap overflow.

https://source.chromium.org/chromium/chromium/src/+/master:components/favicon_base/select_favicon_frames.cc;l=216;drc=e51dd5c377fd47393a171f6bdcd7c1a6a9a609c5;bpv=1;bpt=1

and I find IconHelper::DownloadFaviconCallback may have the same issue.

https://source.chromium.org/chromium/chromium/src/+/master:android_webview/browser/icon_helper.cc;l=71;drc=53d29c2466f83f189e181df6fa692a5659c0be83

VERSION
Chrome Version: [92.0.4481.0] + [x64 dev]
Operating System: [ubuntu 20.10]

REPRODUCTION CASE
1. patch third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
2. python3 -m http.server
3. out/AsanRelease/chrome --user-data-dir=/tmp/noneExists http://localhost:8000/test.html

note:
If browser not crash, please refresh the tab.

FOR CRASHES, PLEASE INCLUDE THE FOLLOWING ADDITIONAL INFORMATION
Type of crash: [browser]
Crash State: [see link above: stack trace *with symbols*, registers, exception record]
Client ID (if relevant): [see link above]

CREDIT INFORMATION
Externally reported security bugs may appear in Chrome release notes. If this bug is included, how would you like to be credited?
Reporter credit: [Anonymous]

render_patch.txt
669 bytes View Download

test.html
133 bytes View Download

youtube.ico
1.1 KB Download

Comment 1 by zhanj...@gmail.com on Wed, Apr 21, 2021, 8:43 PM EDT

asan.txt
21.4 KB View Download

Comment 2 by sheriffbot on Wed, Apr 21, 2021, 8:45 PM EDT Project Member

Labels: external_security_report

Comment 3 by carlosil@chromium.org on Wed, Apr 21, 2021, 9:16 PM EDT Project Member

Cc: carlosil@chromium.org
Labels: Needs-Feedback

It's unclear to me what the issue is here. As the bug seems to be created with the patch. Can you reproduce this without modifying Chrome's code?

Comment 4 by zhanj...@gmail.com on Wed, Apr 21, 2021, 10:43 PM EDT

This is a sandbox issue, trigger it need a compromised renderer, the renderer-side patch render_patch.txt
simulates a compromised renderer state.

Comment 5 by sheriffbot on Wed, Apr 21, 2021, 10:45 PM EDT Project Member

Labels: -Needs-Feedback

Thank you for providing more feedback. Adding the requester to the cc list.

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

Comment 6 by zhanj...@gmail.com on Wed, Apr 21, 2021, 10:51 PM EDT

Sorry, I am not very familiar with Mojo JavaScript Bindings, it's hard for me to write a MojoJS poc html.

Comment 7 by carlosil@chromium.org on Thu, Apr 22, 2021, 10:19 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: hcm@chromium.org
Labels: Security_Impact-Head Security_Severity-High OS-Android OS-Chrome OS-Fuchsia OS-Linux OS-Windows
Components: Internals>Skia

hcm: Can you PTAL and help further triage? Tagging as high severity since this requires a compromised renderer

Comment 8 by zhanj...@gmail.com on Fri, Apr 23, 2021, 12:23 AM EDT

Maybe not skia, but favicon, I think. The root cause is in FaviconHandler::OnDidDownloadFavicon, it should check that 'bitmaps' and 'original_bitmap_sizes' have the same size.

https://source.chromium.org/chromium/chromium/src/+/master:components/favicon/core/favicon_handler.cc;l=503;drc=1bd27d94e27f7e669315e8f30de81f15d27f44ac;bpv=1;bpt=1

```
void FaviconHandler::OnDidDownloadFavicon(
    favicon_base::IconType icon_type,
    int id,
    int http_status_code,
    const GURL& image_url,
    const std::vector<SkBitmap>& bitmaps,
    const std::vector<gfx::Size>& original_bitmap_sizes) {
```

Comment 9 by sheriffbot on Fri, Apr 23, 2021, 12:52 PM EDT Project Member

Labels: M-92 Target-92

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

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

Comment 10 by sheriffbot on Fri, Apr 23, 2021, 1:17 PM EDT Project Member

Labels: ReleaseBlock-Stable

This is a serious security regression. If you are not able to fix this quickly, please revert the change that introduced it.

If this doesn't affect a release branch, or has not been properly classified for severity, please update the Security_Impact or Security_Severity labels, and remove the ReleaseBlock label. To disable this altogether, apply ReleaseBlock-NA.

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

Comment 11 by sheriffbot on Fri, Apr 23, 2021, 1:27 PM EDT 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 12 by zhanj...@gmail.com on Wed, Apr 28, 2021, 8:30 PM EDT

Hello, is someone working on this?

Comment 13 by hcm@google.com on Wed, Apr 28, 2021, 11:50 PM EDT Project Member

Owner: mastiz@chromium.org
Components: -Internals>Skia

as mentioned in earlier comments, it seems the issue may need to be resolved with a check in FaviconHandler... mastiz, do you still work in this code area or can you help assign?

Comment 14 by mastiz@chromium.org on Thu, Apr 29, 2021, 3:33 AM EDT Project Member

Status: Started (was: Assigned)

Favicons are not formally staffed with a team, let me take a quick look.

Comment 15 by mastiz@chromium.org on Thu, Apr 29, 2021, 4:11 AM EDT Project Member

I prepared a patch in https://chromium-review.googlesource.com/c/chromium/src/+/2859102.

I notice there are multiple callers to WebContents::DownloadImage() that could run into similar issues (or at least rely/DCHECK on the two vectors having the same size).

Comment 16 by ajgo@google.com on Thu, Apr 29, 2021, 11:16 AM EDT Project Member

Labels: -Security_Impact-Head Security_Impact-Stable
Components: UI>Browser>History

Adding a component to make my dashboard green, and impact=stable as this code seems to be untouched for a while.

Thanks for looking at this. Should those DCHECKS be CHECKS if the same issue can repeat?

Comment 17 by Git Watcher on Fri, Apr 30, 2021, 3:24 AM EDT Project Member

Status: Fixed (was: Started)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/034ba14e44f08e8ca84b42350f3238f847e08e5f

commit 034ba14e44f08e8ca84b42350f3238f847e08e5f
Author: Mikel Astiz <mastiz@chromium.org>
Date: Fri Apr 30 07:23:49 2021

Guard WebContents::DownloadImage() against malformed renderer response

Callers expect that ImageDownloadCallback gets invoked with two vectors
having the same number of elements (one containing the bitmaps and the
other one the corresponding sizes).

However, these vectors are populated directly from the Mojo response,
so there needs to be some browser-process sanitization to protect
against buggy or compromised renderers.

In this patch, WebContentsImpl::OnDidDownloadImage() mimics a 400 error
if the response is malformed, similarly to how it's done in other edge
cases (renderer process dead upon download). Because this scenario is
a violation of the Mojo API contract, the browser process also issues
a bad message log (newly-introduced WCI_INVALID_DOWNLOAD_IMAGE_RESULT)
and shuts down the renderer process.

Change-Id: I29baa421b3590e9a9eeaee95a6e331c08dce5096
~~Fixed: 1201446~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2859102
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Cr-Commit-Position: refs/heads/master@{#877817}

[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/components/favicon/core/favicon_handler.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/components/favicon/core/favicon_handler.h
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/components/favicon/ios/web_favicon_driver.mm
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/components/favicon_base/select_favicon_frames.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/components/favicon_base/select_favicon_frames.h
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/browser/bad_message.h
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/public/browser/web_contents.h
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/public/test/mock_render_process_host.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/content/test/test_web_contents.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
[modify] https://crrev.com/034ba14e44f08e8ca84b42350f3238f847e08e5f/tools/metrics/histograms/enums.xml

Comment 18 by mastiz@chromium.org on Fri, Apr 30, 2021, 3:40 AM EDT Project Member

NextAction: 2021-05-03

I'll let the above patch bake on canary and consider a merge request into M91 next week.

ajgo@: I don't think this qualifies for CHECKs. Without having had real exploits, it would be hard to draw a line on which callers of WebContents::DownloadImage() should use CHECKs (instead of DCHECKs).

Comment 19 by sheriffbot on Fri, Apr 30, 2021, 12:42 PM EDT Project Member

Labels: reward-topanel

Comment 20 by sheriffbot on Fri, Apr 30, 2021, 2:02 PM EDT Project Member

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

Comment 21 by mastiz@chromium.org on Mon, May 3, 2021, 7:10 AM EDT Project Member

Labels: Merge-Request-91

There's preliminary data only, but I see no crash reports and initial UMA data reports zero instances for the newly-introduced bad message:
https://uma.googleplex.com/p/chrome/histograms?sid=f02e9a2d1c45859875de3c88a5b49439

Requesting merge.

Comment 22 by sheriffbot on Mon, May 3, 2021, 7:13 AM EDT Project Member

Labels: -Merge-Request-91 Hotlist-Merge-Review Merge-Review-91

This bug requires manual review: M91'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), kbleicher@(ChromeOS), pbommana@(Desktop)

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

Comment 23 by mastiz@chromium.org on Mon, May 3, 2021, 7:25 AM EDT Project Member

>. 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

I reached out to Chrome Security for feedback. Meanwhile, my guess is that the issue is severe enough to be merged into Beta (with a few weeks left in the Beta window).

> Links to the CLs you are requesting to merge.
https://chromium-review.googlesource.com/c/chromium/src/+/2859102

> Has the change landed and been verified on ToT?
Yes.

> Does this change need to be merged into other active release branches (M-1, M+1)?
No (?).

> Why are these changes required in this milestone after branch?
It was reported after BP.

> Is this a new feature?
No.

> If it is a new feature, is it behind a flag using finch?
N/A. Semi-related: the fix is NOT behind a feature toggle.

Comment 24 by adetaylor@google.com on Mon, May 3, 2021, 10:54 AM EDT Project Member

Labels: -ReleaseBlock-Stable -M-92 -Target-92 M-91 Target-91 Merge-Request-92

Assuming this is Security_Impact-Stable not Head:
* our normal guidelines would then say M-91
* this isn't a regression so no RBS
* sheriffbot would have requested a merge to M91 as well as M92

So adjusting all the labels thusly.

As for actual merge approvals... I'll take a look later today. (Gut feeling: this feels like quite a complex change to merge back to M91, but on the other hand, it feels like a potentially _really_ easy sandbox escape.)

Comment 25 by adetaylor@chromium.org on Mon, May 3, 2021, 10:57 AM EDT Project Member

Labels: -M-91 -Merge-Request-92 -Target-91 Merge-Request-90 M-90 Target-90

Oops, meant merge-request-90. Will review later today, in any case.

Comment 26 by adetaylor@google.com on Mon, May 3, 2021, 11:09 AM EDT Project Member

Labels: -Merge-Review-91 Merge-Approved-91

Approving merge to M91, please merge to branch 4472.

Comment 27 by mastiz@chromium.org on Mon, May 3, 2021, 2:39 PM EDT Project Member

dcheng@ proposed an interesting follow-up, which I'll take care of: "This is fine, but can we have a followup here to fix the API? Specifically, the Mojo guidelines recommend not to pass parallel arrays for this reason: instead, we should have a struct that groups the image with the original image size, and then pass an array of those."

Comment 28 by Git Watcher on Mon, May 3, 2021, 5:56 PM EDT Project Member

Labels: -merge-approved-91 merge-merged-4472 merge-merged-91

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/00f3335182275f2fd81e363b2daee457774d6690

commit 00f3335182275f2fd81e363b2daee457774d6690
Author: Mikel Astiz <mastiz@chromium.org>
Date: Mon May 03 21:55:28 2021

Guard WebContents::DownloadImage() against malformed renderer response

Callers expect that ImageDownloadCallback gets invoked with two vectors
having the same number of elements (one containing the bitmaps and the
other one the corresponding sizes).

However, these vectors are populated directly from the Mojo response,
so there needs to be some browser-process sanitization to protect
against buggy or compromised renderers.

In this patch, WebContentsImpl::OnDidDownloadImage() mimics a 400 error
if the response is malformed, similarly to how it's done in other edge
cases (renderer process dead upon download). Because this scenario is
a violation of the Mojo API contract, the browser process also issues
a bad message log (newly-introduced WCI_INVALID_DOWNLOAD_IMAGE_RESULT)
and shuts down the renderer process.

(cherry picked from commit 034ba14e44f08e8ca84b42350f3238f847e08e5f)

Change-Id: I29baa421b3590e9a9eeaee95a6e331c08dce5096
~~Fixed: 1201446~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2859102
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Kentaro Hara <haraken@chromium.org>
Commit-Queue: Mikel Astiz <mastiz@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#877817}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2867450
Auto-Submit: Mikel Astiz <mastiz@chromium.org>
Bot-Commit: Rubber Stamper <rubber-stamper@appspot.gserviceaccount.com>
Commit-Queue: Daniel Cheng <dcheng@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Cr-Commit-Position: refs/branch-heads/4472@{#701}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/components/favicon/core/favicon_handler.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/components/favicon/core/favicon_handler.h
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/components/favicon/ios/web_favicon_driver.mm
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/components/favicon_base/select_favicon_frames.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/components/favicon_base/select_favicon_frames.h
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/browser/bad_message.h
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/public/browser/web_contents.h
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/public/test/mock_render_process_host.cc

[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/content/test/test_web_contents.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
[modify] https://crrev.com/00f3335182275f2fd81e363b2daee457774d6690/tools/metrics/histograms/enums.xml

Comment 29 by dcheng@chromium.org on Mon, May 3, 2021, 6:29 PM EDT Project Member

Btw I went and looked at this in a bit more detail, and it appears that we:
- originally had checks
- but lost them when converting them to Mojo

https://codereview.chromium.org/1085783002/diff/140001/content/browser/web_contents/web_contents_impl.cc

So anything we can do to make this more resistant to accidentally losing the check in the future would be good...

Comment 30 by adetaylor@google.com on Tue, May 4, 2021, 12:53 PM EDT Project Member

Labels: -Merge-Request-90 Merge-Approved-90

Approving merge to M90, branch 4430. Please merge by EOD PST Thursday for inclusion in next week's security refresh.

Comment 31 by mastiz@chromium.org on Tue, May 4, 2021, 1:12 PM EDT Project Member

I did take another look at UMA and crashpad and all looks good so far.

Cherry-pick into M90 flight: https://chromium-review.googlesource.com/c/chromium/src/+/2871796

Comment 32 by gov...@chromium.org on Tue, May 4, 2021, 2:11 PM EDT Project Member

Please merge your change to M90 branch 4430 ASAP so we can pick it up for next M90 respin. Thank you.

Comment 33 by mastiz@chromium.org on Tue, May 4, 2021, 3:33 PM EDT Project Member

The cherrypick now has owner approvals but ran into an unrelated test failure (https://bugs.chromium.org/p/chromium/issues/detail?id=1191927). I'll retry the CQ and work it around if necessary.

Comment 34 by Git Watcher on Tue, May 4, 2021, 3:42 PM EDT Project Member

Labels: -merge-approved-90 merge-merged-4430 merge-merged-90

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a

commit 891171c0e9da81c6384cd9a7c3f0b3aadf0c335a
Author: Mikel Astiz <mastiz@chromium.org>
Date: Tue May 04 19:41:16 2021

Guard WebContents::DownloadImage() against malformed renderer response

Callers expect that ImageDownloadCallback gets invoked with two vectors
having the same number of elements (one containing the bitmaps and the
other one the corresponding sizes).

However, these vectors are populated directly from the Mojo response,
so there needs to be some browser-process sanitization to protect
against buggy or compromised renderers.

In this patch, WebContentsImpl::OnDidDownloadImage() mimics a 400 error
if the response is malformed, similarly to how it's done in other edge
cases (renderer process dead upon download). Because this scenario is
a violation of the Mojo API contract, the browser process also issues
a bad message log (newly-introduced WCI_INVALID_DOWNLOAD_IMAGE_RESULT)
and shuts down the renderer process.

(cherry picked from commit 034ba14e44f08e8ca84b42350f3238f847e08e5f)

Change-Id: Ic0843e10efc26809fabd8f1bbe506ba1703d1486
~~Fixed: 1201446~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871796
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Daniel Cheng <dcheng@chromium.org>
Auto-Submit: Mikel Astiz <mastiz@chromium.org>
Cr-Commit-Position: refs/branch-heads/4430@{#1391}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/components/favicon/core/favicon_handler.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/components/favicon/core/favicon_handler.h
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/components/favicon/ios/web_favicon_driver.mm
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/components/favicon_base/select_favicon_frames.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/components/favicon_base/select_favicon_frames.h
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/browser/bad_message.h
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/public/browser/web_contents.h
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/public/test/mock_render_process_host.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/content/test/test_web_contents.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
[modify] https://crrev.com/891171c0e9da81c6384cd9a7c3f0b3aadf0c335a/tools/metrics/histograms/enums.xml

Comment 35 by amyressler@chromium.org on Fri, May 7, 2021, 5:13 PM EDT Project Member

Labels: Release-3-M90

Comment 36 by vsavu@google.com on Mon, May 10, 2021, 9:28 AM EDT Project Member

Labels: LTS-Merge-Request-86 LTS-Security-86

Comment 37 by amyressler@google.com on Mon, May 10, 2021, 9:54 AM EDT Project Member

Labels: CVE-2021-30516 CVE_description-missing

Comment 38 by Git Watcher on Wed, May 12, 2021, 6:53 AM EDT Project Member

Labels: merge-merged-4430_101

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/817a17616877f01b4c30ac498ee20ca74efb6d4e

commit 817a17616877f01b4c30ac498ee20ca74efb6d4e
Author: Mikel Astiz <mastiz@chromium.org>
Date: Wed May 12 10:52:10 2021

Guard WebContents::DownloadImage() against malformed renderer response

Callers expect that ImageDownloadCallback gets invoked with two vectors
having the same number of elements (one containing the bitmaps and the
other one the corresponding sizes).

However, these vectors are populated directly from the Mojo response,
so there needs to be some browser-process sanitization to protect
against buggy or compromised renderers.

In this patch, WebContentsImpl::OnDidDownloadImage() mimics a 400 error
if the response is malformed, similarly to how it's done in other edge
cases (renderer process dead upon download). Because this scenario is
a violation of the Mojo API contract, the browser process also issues
a bad message log (newly-introduced WCI_INVALID_DOWNLOAD_IMAGE_RESULT)
and shuts down the renderer process.

(cherry picked from commit 034ba14e44f08e8ca84b42350f3238f847e08e5f)

(cherry picked from commit 891171c0e9da81c6384cd9a7c3f0b3aadf0c335a)

Change-Id: Ic0843e10efc26809fabd8f1bbe506ba1703d1486
~~Fixed: 1201446~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871796
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Daniel Cheng <dcheng@chromium.org>
Auto-Submit: Mikel Astiz <mastiz@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1391}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2884072
Owners-Override: Victor-Gabriel Savu <vsavu@google.com>
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4430_101@{#24}
Cr-Branched-From: 3e9034a21f4b1f6707146b1309e001c3321ab48a-refs/branch-heads/4430@{#1364}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/components/favicon/core/favicon_handler.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/components/favicon/core/favicon_handler.h
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/components/favicon/ios/web_favicon_driver.mm
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/components/favicon_base/select_favicon_frames.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/components/favicon_base/select_favicon_frames.h
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/browser/bad_message.h
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/public/browser/web_contents.h
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/public/test/mock_render_process_host.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/content/test/test_web_contents.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
[modify] https://crrev.com/817a17616877f01b4c30ac498ee20ca74efb6d4e/tools/metrics/histograms/enums.xml

Comment 39 by gianluca@google.com on Wed, May 12, 2021, 12:29 PM EDT Project Member

Labels: -LTS-Merge-Request-86 LTS-Merge-Approved-86

Comment 40 by amyressler@google.com on Wed, May 12, 2021, 7:12 PM EDT 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 41 by amyressler@chromium.org on Wed, May 12, 2021, 7:31 PM EDT Project Member

Congratulations on another one! The VRP Panel has decided to award you $20,000 for this report. Very excellent work!

Comment 42 by amyressler@google.com on Mon, May 17, 2021, 2:16 PM EDT Project Member

Labels: -reward-unpaid reward-inprocess

Comment 43 by Git Watcher on Thu, May 20, 2021, 12:14 PM EDT Project Member

Labels: merge-merged-4240

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/fdc766beb82656461fb07703196bafc1f23b9c68

commit fdc766beb82656461fb07703196bafc1f23b9c68
Author: Mikel Astiz <mastiz@chromium.org>
Date: Thu May 20 16:13:40 2021

[M86-LTS]: Guard WebContents::DownloadImage() against malformed renderer response

Callers expect that ImageDownloadCallback gets invoked with two vectors
having the same number of elements (one containing the bitmaps and the
other one the corresponding sizes).

However, these vectors are populated directly from the Mojo response,
so there needs to be some browser-process sanitization to protect
against buggy or compromised renderers.

In this patch, WebContentsImpl::OnDidDownloadImage() mimics a 400 error
if the response is malformed, similarly to how it's done in other edge
cases (renderer process dead upon download). Because this scenario is

a violation of the Mojo API contract, the browser process also issues
a bad message log (newly-introduced WCI_INVALID_DOWNLOAD_IMAGE_RESULT)
and shuts down the renderer process.

[M86]: fixed trivial conflicts
    test_web_contents.cc moved to calling OnDidDownloadImage like http://crrev.com/c/2520236
    Added missing include to web_contents_impl_unittest.cc
(cherry picked from commit 034ba14e44f08e8ca84b42350f3238f847e08e5f)

(cherry picked from commit 891171c0e9da81c6384cd9a7c3f0b3aadf0c335a)

Change-Id: Ic0843e10efc26809fabd8f1bbe506ba1703d1486
~~Fixed: 1201446~~
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2871796
Reviewed-by: Avi Drissman <avi@chromium.org>
Reviewed-by: Daniel Cheng <dcheng@chromium.org>
Commit-Queue: Daniel Cheng <dcheng@chromium.org>
Auto-Submit: Mikel Astiz <mastiz@chromium.org>
Cr-Original-Commit-Position: refs/branch-heads/4430@{#1391}
Cr-Original-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2883703
Reviewed-by: Achuith Bhandarkar <achuith@chromium.org>
Owners-Override: Jana Grill <janagrill@google.com>
Commit-Queue: Victor-Gabriel Savu <vsavu@google.com>
Cr-Commit-Position: refs/branch-heads/4240@{#1646}
Cr-Branched-From: f297677702651916bbf65e59c0d4bbd4ce57d1ee-refs/heads/master@{#800218}

[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/components/favicon/core/favicon_handler.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/components/favicon/core/favicon_handler.h
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/components/favicon/ios/web_favicon_driver.mm
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/components/favicon_base/select_favicon_frames.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/components/favicon_base/select_favicon_frames.h
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/browser/bad_message.h
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/browser/web_contents/web_contents_impl.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/browser/web_contents/web_contents_impl.h
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/browser/web_contents/web_contents_impl_unittest.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/public/browser/web_contents.h
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/public/test/mock_render_process_host.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/content/test/test_web_contents.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/third_party/blink/renderer/modules/image_downloader/image_downloader_impl.cc
[modify] https://crrev.com/fdc766beb82656461fb07703196bafc1f23b9c68/tools/metrics/histograms/enums.xml

Comment 44 by amyressler@google.com on Fri, Jun 4, 2021, 7:23 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 45 by sheriffbot on Thu, Aug 26, 2021, 1:30 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