





☆ Starred by 2 users

Owner:	 <a href="#">gambard@chromium.org</a> <b>OOO til Dec. 20</b>
CC:	<a href="#">rakurati@chromium.org</a> <a href="#">adetaylor@chromium.org</a> <a href="#">rsesek@chromium.org</a>  <a href="#">ajuma@chromium.org</a> <a href="#">est...@chromium.org</a> <a href="#">eugen...@chromium.org</a> <a href="#">subha...@chromium.org</a>  <a href="#">justincohen@chromium.org</a> <a href="#">linds...@chromium.org</a> <a href="#">achuith@chromium.org</a> <a href="#">srikanthg@chromium.org</a> <a href="#">rohitrao@chromium.org</a>  <a href="#">khorimoto@chromium.org</a> <a href="#">ios-bugs-priority@chromium.org</a> <a href="#">ios-bugs@chromium.org</a>
Status:	Fixed (Closed)
Components:	Mobile>iOSWeb>Security
Modified:	May 6, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	iOS
Pri:	1
Type:	Bug-Security
<div>reward-500</div> <div>Security_Impact-Stable</div> <div>Security_Severity-Medium</div> <div>allpublic</div> <div>reward-inprocess</div> <div>CVE_description-submitted</div> <div>Target-79</div> <div>M-79</div> <div>Release-0-M80</div> <div>CVE-2020-6403</div>	

**Issue 1006012: Security: URL bar spoofing on iOS**  
Reported by [chrom...@gmail.com](#) on Thu, Sep 19, 2019, 7:14 PM EDT

 Code

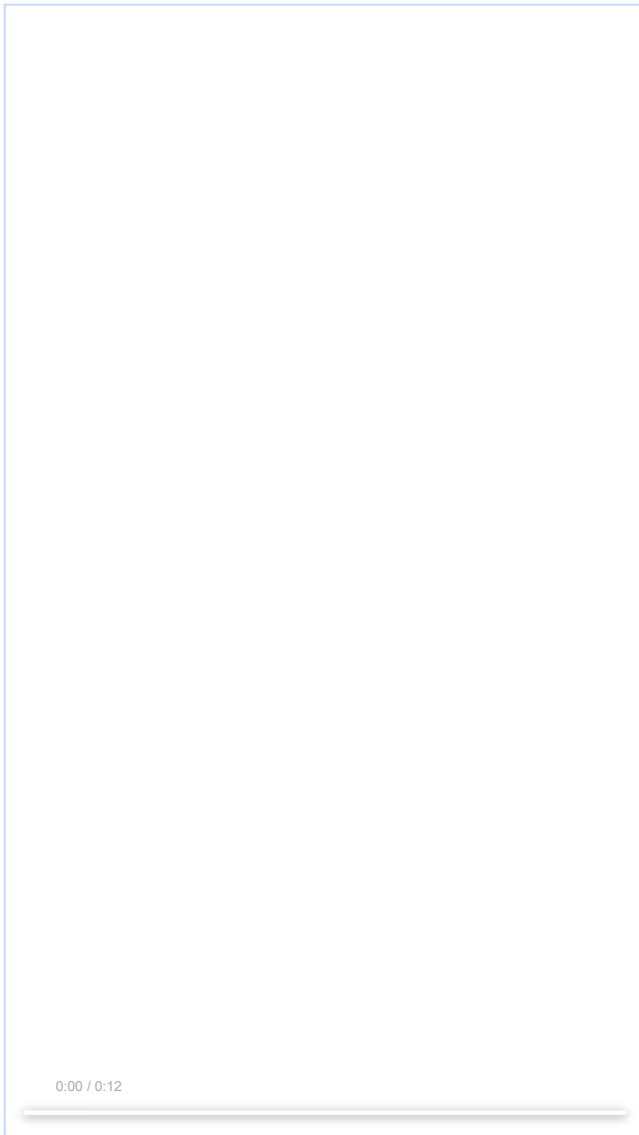
**VERSION**  
Chrome Version: 78.0.3904.20  
Operating System: iOS

**REPRODUCTION CASE**  
1. Lunch the PoC  
2. Click on the button to copy the link  
3. Focus the address bar and past the link  
4. Click on the link to stop pending

**poc.html**  
673 bytes [View](#) [Download](#)

Comment 1 by [chrom...@gmail.com](#) on Thu, Sep 19, 2019, 7:23 PM EDT

**6199AB97-2C3F-424F-8756-60F9C9AE4FDD.MP4**  
499 KB [View](#) [Download](#)



[Deleted] **E63D39A9-C524-45E8-896D-8DA163093613.MP4**

[Comment 2](#) by [rsesek@chromium.org](mailto:rsesek@chromium.org) on Fri, Sep 20, 2019, 2:11 PM EDT

**Owner:** [mrsuyi@chromium.org](mailto:mrsuyi@chromium.org)

**Cc:** [ajuma@chromium.org](mailto:ajuma@chromium.org) [gambard@chromium.org](mailto:gambard@chromium.org) [justincohen@chromium.org](mailto:justincohen@chromium.org) [eugen...@chromium.org](mailto:eugen...@chromium.org) [rohitrato@chromium.org](mailto:rohitrato@chromium.org) [kkhorimoto@chromium.org](mailto:kkhorimoto@chromium.org)

**Labels:** Security\_Severity-Medium Security\_Impact-Beta M-78 OS-iOS Pri-1

**Components:** Mobile>IOSWeb>Security

[mrsuyi](#): Could you take a look? I don't have a device to try and repro this.

[Comment 3](#) by [justincohen@chromium.org](mailto:justincohen@chromium.org) on Fri, Sep 20, 2019, 2:44 PM EDT

**Cc:** [rsesek@chromium.org](mailto:rsesek@chromium.org)

This reproduces with SlimNav both off an on, and on Safari too.

Chrome shows the pending url [google.com](http://google.com) with the old content, and then after 60 seconds reverts to showing the poc URL. Chrome stops showing the loading bar after tapping the second link. Chrome does not alert when tapping an invalid protocol url.

Safari also shows '[google.com](http://google.com)' in the omnibox (it's pending), but they also display an alert saying the second link address is invalid. After dismissing the alert, Safari still shows [google.com](http://google.com) with the old content, and then replaces the content with a 'stopped responding' page after 60 seconds. Safari also stops showing the loading bar after tapping the second link.

The difference seems to be Chrome reverts to showing the poc page and url, Safari eventually shows [google.com](http://google.com) with a stopped responding page.

What is the correct thing to do here? It is correct that we show [google.com](http://google.com) while it's pending, and still trying to load. Perhaps it's just not that the loading progress bar or spinner aren't displayed? Safari also doesn't show this.

If you don't tap on the link, Chrome eventually shows the 'site cannot be reached' error, so perhaps that's the bug?

Should chrome display alerts for invalid protocols? Is not doing that part of the bug, or just not showing the spinner?

[rsesek@](#) wdyt? I think this is probably low severity. I'm not sure what is correct here...

[Comment 4](#) by [rsesek@chromium.org](mailto:rsesek@chromium.org) on Fri, Sep 20, 2019, 3:06 PM EDT

**Cc:** [est...@chromium.org](mailto:est...@chromium.org)

Thanks for taking a look. I agree it makes some sense for the address bar to show the pending load, but it should probably revert after it fails.

But this is really a question for Enamel, so CC +estark.

Regarding Sev-Low, I think this could be downgraded but our severity guidelines do put spoofs at Medium. I'll let Enamel decide.

[Comment 5](#) by [justincohen@chromium.org](mailto:justincohen@chromium.org) on Fri, Sep 20, 2019, 3:13 PM EDT

> but it should probably revert after it fails.

...it does revert after it fails. I don't know why we don't show the loading bar anymore (like safari) or why we revert to the old page rather than show the failure page (different from safari).

[Comment 6](#) by [rsesek@chromium.org](mailto:rsesek@chromium.org) on Fri, Sep 20, 2019, 3:21 PM EDT

Sorry, I wrote "revert" when I meant "show the error page," since it seems like a failed navigation.

[Comment 7](#) by [justincohen@chromium.org](mailto:justincohen@chromium.org) on Fri, Sep 20, 2019, 3:26 PM EDT

[rsesek@](mailto:rsesek@) agreed

[estark@](#) unsure if there's a security implication here, since the end result is either 'show error page with google in omnibox' or 'revert to poc url with old content'.

Not showing the progress bar might be worth filing a radar depending on the cause.

[Comment 8](#) by [est...@chromium.org](mailto:est...@chromium.org) on Fri, Sep 20, 2019, 4:58 PM EDT

Agree with severity Medium, since this is a reasonably convincing spoof with some mitigations. (Convincing spoof with no mitigations would be High.)

Showing an error page seems like the right thing to do IMO.

[Comment 9](#) by [justincohen@chromium.org](mailto:justincohen@chromium.org) on Fri, Sep 20, 2019, 5:36 PM EDT

[@estark](#), per offline conversation, can you link to a bug on differentiating pending vs committed urls? It sounds like the lack of a progress bar is the spoof, and the not showing error page is a bug, but maybe not a spoof. Do you agree?

[Comment 10](#) by [est...@chromium.org](mailto:est...@chromium.org) on Fri, Sep 20, 2019, 6:35 PM EDT

Agree with #9. It doesn't look like we have an open bug for differentiating pending vs committed URLs, but it's discussed in <https://bugs.chromium.org/p/chromium/issues/detail?id=719856#c11> and a number of bugs linked from that thread.

[Comment 11](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Sat, Sep 21, 2019, 10:02 AM EDT

**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 12](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Sat, Sep 21, 2019, 11:17 AM EDT

**Status:** Assigned (was: Unconfirmed)

[Comment 13](#) by [mrsuyi@chromium.org](mailto:mrsuyi@chromium.org) on Mon, Sep 23, 2019, 5:54 AM EDT

**Labels:** Restrict-View-Google

Here is what happens:

1. User loads <https://www.google.com:1234/> in omnibox;
2. KVO of WKWebView.URL=<https://www.google.com:1234/> and WKWebView.loading=true are invoked;
3. WebStateImpl::IsLoading is set to true;
3. "decidePolicyForNavigationAction" and "didStartProvisionalNavigation" are invoked for <https://www.google.com:1234/>;
4. User taps on the link of <https://www.verylongurl.googlecloudplatform.accounts.google.com> in the page;
5. "decidePolicyForNavigationAction" is invoked for <https://www.verylongurl.googlecloudplatform.accounts.google.com>, with WKWebView.URL=<https://www.google.com:1234/>, and reaches here: [https://cs.chromium.org/chromium/src/ios/web/navigation/crw\\_wk\\_navigation\\_handler.mm?rcl=644d8a647b02c897606f5b5f55f6da0584af3c899&l=382](https://cs.chromium.org/chromium/src/ios/web/navigation/crw_wk_navigation_handler.mm?rcl=644d8a647b02c897606f5b5f55f6da0584af3c899&l=382)
6. WebStateImpl::IsLoading is set to false which emits a "webStateDidStopLoading" event to ToolbarMediator and hides the progress bar: [https://cs.chromium.org/chromium/src/ios/chrome/browser/ui/toolbar/toolbar\\_mediator.mm?rcl=644d8a647b02c897606f5b5f55f6da0584af3c899&l=130](https://cs.chromium.org/chromium/src/ios/chrome/browser/ui/toolbar/toolbar_mediator.mm?rcl=644d8a647b02c897606f5b5f55f6da0584af3c899&l=130)

The root cause here is that WebState::IsLoading is set to false while WKWebView.loading==true. I think only updating WebState::IsLoading in KVO of WKWebView.loading will fix this bug, and here is a design doc about it:

[https://docs.google.com/document/d/12lhr6zfv60IMXAFQuKpSh3eFs35s\\_pHF51a-Zujg/edit?usp=sharing](https://docs.google.com/document/d/12lhr6zfv60IMXAFQuKpSh3eFs35s_pHF51a-Zujg/edit?usp=sharing)

However that change will probably take a long time to be landed, and I don't have a feasible solution only for this bug right now.

[Comment 14](#) by [kariahda@google.com](mailto:kariahda@google.com) on Tue, Oct 1, 2019, 9:56 AM EDT

**Cc:** [adetaylor@chromium.org](mailto:adetaylor@chromium.org)

[estark](#), [+adetaylor](#)

Please see c13. It looks like there is no feasible solution for this bug for M78, and RBS was added by sheriffbot in c11 after some investigations.

Please confirm it's ok to "not" have this fixed in M78 stable.

[Comment 15](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Tue, Oct 1, 2019, 2:04 PM EDT

[justincohen@](#), can you confirm whether this bug has been around forever, or was introduced in M78? From [#c3](#) it sounds like it might have been around for a while, in which case I'll adjust Security\_Impact and remove the RBS flag. (RBS was added by Sheriffbot on the grounds that this is a regression).

[Comment 16](#) by [justincohen@chromium.org](mailto:justincohen@chromium.org) on Tue, Oct 1, 2019, 3:55 PM EDT

[adetaylor@](#) This is not a new issue.

[Comment 17](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Wed, Oct 2, 2019, 3:52 PM EDT

**Labels:** -Security\_Impact-Beta -ReleaseBlock-Stable Security\_Impact-Stable

Thanks.

[Comment 18](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Mon, Oct 7, 2019, 9:10 AM EDT

[mrsuyi](#): Uh oh! This issue still open and hasn't been updated in the last 14 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

[Comment 19](#) by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Tue, Oct 22, 2019, 9:10 AM EDT

[mrsuyi](#): Uh oh! This issue still open and hasn't been updated in the last 29 days. This is a serious vulnerability, and we want to ensure that there's progress. Could you please leave an update with the current status and any potential blockers?

If you're not the right owner for this issue, could you please remove yourself as soon as possible or help us find the right one?

If the issue is fixed or you can't reproduce it, please close the bug. If you've started working on a fix, please set the status to Started.

Thanks for your time! To disable nags, add the Disable-Nags label.

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

**Comment 20** by [mrsuyi@chromium.org](mailto:mrsuyi@chromium.org) on Thu, Oct 31, 2019, 12:23 PM EDT

**Cc:** [srikanthg@chromium.org](mailto:srikanthg@chromium.org)

**Comment 21** by [mrsuyi@chromium.org](mailto:mrsuyi@chromium.org) on Thu, Oct 31, 2019, 1:07 PM EDT

**Cc:** [linds...@chromium.org](mailto:linds...@chromium.org)

**Comment 22** Deleted

**Comment 23** by [gambard@chromium.org](mailto:gambard@chromium.org) on Tue, Nov 12, 2019, 11:00 AM EST

**Cc:** [subha...@chromium.org](mailto:subha...@chromium.org)

**Comment 24** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Wed, Dec 11, 2019, 9:12 AM EST

**Labels:** -M-78 Target-79 M-79

**Comment 25** by [gambard@chromium.org](mailto:gambard@chromium.org) on Wed, Dec 11, 2019, 9:52 AM EST

estark@, 3 questions:

1. When the user tap on the invalid link (e.g. <https://>), is the correct behavior to display an alert saying "Trying to access invalid URL" (as the other browsers do)?
2. When a navigation fails because it was cancelled (as it is the case for the first navigation here after 60s and tapping on the invalid link), should we display and error page or revert back to the original page & URL?
3. Do we need to fix both of above two questions to mark this bug as fix or can we mark this bug as fixed once the spoofing issue is resolved and do the other changes separately?

**Comment 26** by [gambard@chromium.org](mailto:gambard@chromium.org) on Fri, Dec 13, 2019, 10:33 AM EST

estark@: ping

**Comment 27** by [est...@chromium.org](mailto:est...@chromium.org) on Fri, Dec 13, 2019, 4:19 PM EST

Re #25:

1. That sounds fine from a security perspective, but you might want to check with UX.
2. Either one sounds fine to me from a security perspective; what do we do on other platforms? Reverting back to the original page and URL sounds slightly more natural to me.
3. I think once the spoof is fixed, we can mark this as fixed and file a separate bug for the other non-security changes.

**Comment 28** by [gambard@chromium.org](mailto:gambard@chromium.org) on Mon, Dec 16, 2019, 5:13 AM EST

Thanks!

1. I have checked with UX, they would prefer a popup indicating an incorrect URL (on desktop we don't show anything)
2. On desktop we have the same behavior (i.e. reverting to the original URL). I think it is probably the best.
3. Thanks. This is rolling out as an experiment, the bug will be marked as fixed once we reach 100%.

**Comment 29** by [mrsuyi@chromium.org](mailto:mrsuyi@chromium.org) on Mon, Dec 16, 2019, 10:26 AM EST

**Owner:** [gambard@chromium.org](mailto:gambard@chromium.org)

**Cc:** [gambard@chromium.org](mailto:gambard@chromium.org)

**Comment 30** by [subha...@chromium.org](mailto:subha...@chromium.org) on Tue, Jan 14, 2020, 5:31 AM EST

Tested on:

App Version: 80.0.3987.50 beta  
Devices: iPhone 6 Plus, iPhone XS  
iOS Versions: 12.4.2, 13.3.1 Beta

Issue is fixed with feature flag #use-WKWebView-loading. Chrome shows the pending URL [google.com](https://google.com) with the old content and loading bar when the navigation expires after tapping on the incorrect link, it reverts to the original page and URL.

**Comment 31** by [chrom...@gmail.com](mailto:chrom...@gmail.com) on Thu, Jan 16, 2020, 9:32 AM EST

Verified on 80.0.3987.42 beta. Fixed.

**Comment 32** by [chrom...@gmail.com](mailto:chrom...@gmail.com) on Mon, Jan 20, 2020, 12:28 PM EST

Is this should be marked as "Fixed"?

**Comment 33** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Tue, Jan 21, 2020, 11:38 AM EST

[gambard@chromium.org](mailto:gambard@chromium.org) did you commit a fix here? Or was this fixed by another change? If the latter, please figure out the relevant crbug and mark this one as a duplicate, so we can ensure reporters are credited properly in release notes. Thanks.

**Comment 34** by [gambard@chromium.org](mailto:gambard@chromium.org) on Tue, Jan 28, 2020, 6:20 AM EST

**Status:** Fixed (was: Assigned)

Closing this. It is rolling out via Finch and will be enabled by default soon.  
Thanks for your patience.

**Comment 35** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Tue, Jan 28, 2020, 12:17 PM EST

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

**Comment 36** by [adetaylor@google.com](mailto:adetaylor@google.com) on Thu, Jan 30, 2020, 6:48 PM EST

[gambard@chromium.org](mailto:gambard@chromium.org) per #c33 I'm going to need a bit more help from you to make sure this is properly credited in the release notes and a CVE allocated. Will this be fixed in the initial release of M80? (Whether by Finch or code change.)

**Comment 37** by [gambard@chromium.org](mailto:gambard@chromium.org) on Fri, Jan 31, 2020, 2:43 AM EST

The goal is to ramp up from 1% to 100% via Finch in M80.

**Comment 38** by [adetaylor@google.com](mailto:adetaylor@google.com) on Sat, Feb 1, 2020, 8:14 PM EST

**Labels:** Release-0-M80

Thanks. I'll credit it on M80 then.

**Comment 39** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Mon, Feb 3, 2020, 12:31 PM EST

**Labels:** reward-topanel

**Comment 40** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Mon, Feb 3, 2020, 12:39 PM EST

**Labels:** Merge-Request-80

This is sufficiently serious that it should be merged to beta. But I can't see a Chromium repo commit here, so you will need to investigate what - if anything - needs to be merged to M80. Is there a fix in some other repo which should be merged? Or, perhaps this ticket is a duplicate of some other ticket which has the real fix: please track that down and ensure it is merged appropriately.

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

**Comment 41** by [sheriffbot@chromium.org](mailto:sheriffbot@chromium.org) on Mon, Feb 3, 2020, 12:43 PM EST

**Labels:** -Merge-Request-80 Merge-Review-80 Hotlist-Merge-Review

This bug requires manual review: Less than -2 days to go before AppStore submit on M80  
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://goto.google.com/chrome-release-branch-merge-guidelines>  
- 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 master/TotT?
4. Why are these changes required in this milestone after branch?
5. Is this a new feature?
6. If it is a new feature, is it behind a flag using finch?

Please contact the milestone owner if you have questions.

Owners: govind@(Android), Kariahda@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

**Comment 42** by [gambard@chromium.org](mailto:gambard@chromium.org) on Mon, Feb 3, 2020, 2:48 PM EST

**Labels:** -Hotlist-Merge-Review -Merge-Review-80

**Comment 43** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 3, 2020, 6:47 PM EST

**Labels:** CVE-2020-6403 CVE\_description-missing

**Comment 44** by [awhalley@google.com](mailto:awhalley@google.com) on Tue, Feb 4, 2020, 11:36 PM EST

Hi mrsuyi@ - some other Chromium embedders are interested in this bug now it's been included in M80 release notes. Is Restrict-View-Google from [Comment 13](#) still needed (given the doc link will remain Google only) Thanks.

**Comment 45** by [gambard@chromium.org](mailto:gambard@chromium.org) on Wed, Feb 5, 2020, 3:31 AM EST

**Labels:** -Restrict-View-Google

I removed the Restrict-View-Google.

**Comment 46** by [subha...@chromium.org](mailto:subha...@chromium.org) on Wed, Feb 5, 2020, 6:28 AM EST

**Cc:** [rakurati@chromium.org](mailto:rakurati@chromium.org)

**Comment 47** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Feb 5, 2020, 6:58 PM EST

**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](mailto:security-vrp@chromium.org) with any questions.

\*\*\*\*\*

**Comment 48** by [pabrai@chromium.org](mailto:pabrai@chromium.org) on Wed, Feb 5, 2020, 7:05 PM EST

Congrats the Panel decided to award \$500 for this report!

**Comment 49** by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Wed, Feb 5, 2020, 7:13 PM EST

**Labels:** -reward-unpaid reward-inprocess

**Comment 50** by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Mon, Feb 10, 2020, 4:37 PM EST

**Labels:** -CVE\_description-missing CVE\_description-submitted

**Comment 51** by [bugdroid](mailto:bugdroid) on Thu, Feb 27, 2020, 2:59 AM EST

The following revision refers to this bug:  
<https://chromium.googlesource.com/chromium/src.git/+9a85728692b46f719dd2b0df05da5fbc93c7880>

commit [9a85728692b46f719dd2b0df05da5fbc93c7880](https://chromium.googlesource.com/chromium/src.git/+9a85728692b46f719dd2b0df05da5fbc93c7880)

Author: Gauthier Ambard <[gambard@chromium.org](mailto:gambard@chromium.org)>

Date: Thu Feb 27 07:56:08 2020

[iOS] Cleanup after using WK loading

This CL removes the code that was doing the switch for the feature to use the WKWebView loading property.  
The property is enabled to 100%.

**Bug:** [1006012\\_767092](#)

Change-Id: [Id4a4ca3ad18b24cb97e79c32aece943470d9d0a5](#)

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+2074641>

Auto-Submit: Gauthier Ambard <[gambard@chromium.org](mailto:gambard@chromium.org)>

Reviewed-by: Eugene But <[eugenebut@chromium.org](mailto:eugenebut@chromium.org)>

Commit-Queue: Gauthier Ambard <[gambard@chromium.org](mailto:gambard@chromium.org)>

Cr-Commit-Position: refs/heads/master@{#744967}

[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/about\\_flags.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/about_flags.mm)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/ios\\_chrome\\_flag\\_descriptions.cc](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/ios_chrome_flag_descriptions.cc)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/ios\\_chrome\\_flag\\_descriptions.h](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/flags/ios_chrome_flag_descriptions.h)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/ui/tab\\_grid/tab\\_grid\\_mediator\\_unittest.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/chrome/browser/ui/tab_grid/tab_grid_mediator_unittest.mm)  
[modify] <https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/common/features.h>  
[modify] <https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/common/features.mm>  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/crw\\_web\\_view\\_navigation\\_observer.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/crw_web_view_navigation_observer.mm)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/crw\\_web\\_navigation\\_handler.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/crw_web_navigation_handler.mm)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/wk\\_based\\_navigation\\_manager\\_impl.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/navigation/wk_based_navigation_manager_impl.mm)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/web\\_state/ui/crw\\_web\\_controller.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbc93c7880/ios/web/web_state/ui/crw_web_controller.mm)

[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbce93c7880/ios/web/web\\_state/ui/crw\\_web\\_request\\_controller.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbce93c7880/ios/web/web_state/ui/crw_web_request_controller.mm)  
[modify] [https://crrev.com/9a85728692b46f719dd2b0df05da5fbce93c7880/ios/web/web\\_state/web\\_state\\_observer\\_inttest.mm](https://crrev.com/9a85728692b46f719dd2b0df05da5fbce93c7880/ios/web/web_state/web_state_observer_inttest.mm)

Comment 52 by [adetaylor@google.com](mailto:adetaylor@google.com) on Wed, Mar 4, 2020, 1:43 PM EST

Cc: [achuith@chromium.org](mailto:achuith@chromium.org)

Comment 53 by [sheriffbot](#) on Wed, May 6, 2020, 2:55 PM EDT

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