




☆ Starred by 1 user

**Owner:** [est...@chromium.org](#)

**CC:** [davidben@chromium.org](#)  
[wjmaclean@chromium.org](#)  
[fsam...@chromium.org](#)  
 [jww@chromium.org](#)  
 [rsleeve@chromium.org](#)  
[nhar...@chromium.org](#)  
[nparker@chromium.org](#)  
 [mknowles@chromium.org](#)  
[sporeba@google.com](#)  
[stefanoduo@google.com](#)

**Status:** Fixed (Closed)

**Components:** [Internals>Network>SSL](#)  
[UI>Browser>Interstitials](#)

**Modified:** Sep 3, 2020

**Backlog-Rank:** ----

**Editors:** ----

**EstimatedDays:** ----

**NextAction:** ----

**OS:** [Linux](#), [Android](#), [Windows](#), [Chrome](#), [Mac](#), [Fuchsia](#)

**Pri:** 2

**Type:** [Bug](#)-Security

[reward-500](#)  
[Via-Wizard](#)  
[Security\\_Severity-Low](#)  
[Security\\_Impact-Stable](#)  
[reward-decline](#)  
[allpublic](#)  
[CVE\\_description-submitted](#)  
[Target-77](#)  
[Target-78](#)  
[Target-79](#)  
[M-79](#)  
[M-81](#)  
[Release-0-M81](#)  
[CVE-2020-6437](#)  
[Team-Security-UX](#)  
[Team-TrustyTransport](#)

## Issue 639173: ignored TLS errors propagate from webview to main browser

Reported by [jannhorn@googlemail.com](#) on Thu, Aug 18, 2016, 10:11 PM EDT

 Code

UserAgent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36

Steps to reproduce the problem:

1. Add the attached app to Chrome. Note that it does not request any user-visible permissions.
2. Go to <https://37.221.195.125/>. You'll see the TLS error screen (because the hostname doesn't match the cert); do "not" click through it.
3. Open the newly installed app. You'll see the TLS error screen again, but this time half-transparent and green because it's coming from inside a webview with CSS styles.
4. Click through the half-transparent TLS error screen.
5. Now try loading <https://37.221.195.125/> in the main browser window again.

What is the expected behavior?  
The main browser window should still show a TLS error.

What went wrong?  
Apparently the state of ignored TLS errors is shared between webviews and normal browser tabs?

I believe that this is a problem because, as shown, an app without any visible permissions can perform clickjacking attacks against TLS error screens.

Did this work before? N/A

Chrome version: 52.0.2743.116 Channel: stable  
OS Version:  
Flash Version: Shockwave Flash 22.0 r0

I guess this is low severity because it only works from app context, it requires user interaction and it's useless without a MITM position on the network?

In case this qualifies for a reward: I'm not sure whether I'm eligible to receive rewards.

**webview-tls-test.crx**  
1.5 KB [Download](#)

**webview-tls-test.zip**  
1.4 KB [Download](#)

Comment 1 by [jialiul@chromium.org](#) on Fri, Aug 19, 2016, 2:09 PM EDT Project Member

Cc: [f...@chromium.org](#)

Personally, I feel friction is pretty high to make the attack successful. And if an extension/app really did something bad, it will be removed and blocked. Unless the attacker has access to the victim's browser and install the bad app via Developer mode. But if that's the case, much worse things can be done.

+felt@, what do you think about this one? Should I fold it into [bug-309354?](#)

Comment 2 by [infe...@chromium.org](#) on Tue, Aug 23, 2016, 10:58 AM EDT Project Member

**Status:** Assigned (was: Unconfirmed)  
**Owner:** f...@chromium.org  
**Cc:** -f...@chromium.org

Adrienne, can you please help to triage. Thanks!

[Comment 3](#) by f...@chromium.org on Mon, Aug 29, 2016, 10:41 AM EDT Project Member

**Cc:** jww@chromium.org nparker@chromium.org rsleevi@chromium.org  
**Components:** Security>UX Internals>Network>SSL

It seems like there are two issues here:

A) Is it OK that we are sharing exception state between the app's WV and the rest of Chrome?

My opinion: this is undesirable, even outside of the clickjacking issue. The context of an app seems different enough to me that I would expect it to have its own state. However, I suspect we do connection pooling etc across apps and regular tabs.

Adding sleevi and jww to chime in on this issue.

=====

B) Is it OK that an app can modify the appearance and state of an interstitial inside a WebView?

This seems WAI to me in theory. WVs are meant to be controllable by the embedder. However, combined with (A) it does seem like undesirable behavior.

Adding nparker since he's thought about interstitials in WVs in the past.

[Comment 4](#) by f...@chromium.org on Mon, Aug 29, 2016, 10:43 AM EDT Project Member

In terms of whether this is a security bug, the threshold for making a successful attack is very high. The attacker needs to:

- Achieve a privileged network position (to accomplish MITM)
- Trick the user into installing the app
- Mount this clickjacking attack

Altogether, this doesn't seem like a promising attack vector and I'd say it's low-severity in terms of our triage guidelines. I do agree that there is a problem here though.

[Comment 5](#) by rsleevi@chromium.org on Mon, Aug 29, 2016, 4:44 PM EDT Project Member

Adrienne: The privileged network connection doesn't seem a very high bar (c.f. [http://web.eecs.umich.edu/~zhiyunq/tcp\\_sequence\\_number\\_inference/](http://web.eecs.umich.edu/~zhiyunq/tcp_sequence_number_inference/)), but I would suggest this represents a larger issue, and is perhaps an unresolved manifestation of [issue-2014417](#) that was missed.

[Comment 6](#) by rsleevi@chromium.org on Mon, Aug 29, 2016, 4:45 PM EDT Project Member

Paper link: [http://www.cs.ucr.edu/~zhiyunq/pub/sec16\\_TCP\\_pure\\_offpath.pdf](http://www.cs.ucr.edu/~zhiyunq/pub/sec16_TCP_pure_offpath.pdf)

[Comment 7](#) by f...@chromium.org on Mon, Aug 29, 2016, 9:02 PM EDT Project Member

**Cc:** nhar...@chromium.org

+nharper, since it seems like this is related to [issue-2014417](#)

[Comment 8](#) by wfh@chromium.org on Wed, Sep 7, 2016, 3:44 PM EDT Project Member

**Labels:** Security\_Severity-Low Security\_Impact-Stable

[Comment 9](#) by f...@chromium.org on Fri, Sep 9, 2016, 6:43 PM EDT Project Member

**Owner:** nhar...@chromium.org  
**Cc:** -nhar...@chromium.org f...@chromium.org

nharper, ptal?

[Comment 10](#) by rsleevi@chromium.org on Fri, Sep 9, 2016, 6:59 PM EDT Project Member

**Status:** Untriaged (was: Assigned)  
**Owner:** a\_deleted\_user  
**Cc:** -f...@chromium.org wjmaclea@chromium.org nhar...@chromium.org

I'm not sure why Nick got added - this is not caused by [issue-2014417](#), just yet another manifestation of holding //net wrong. Nick's investigation was prompted by reducing Channel ID mismatches, but the //net team isn't a good owner for this - this is well beyond our ken and about how people are holding //net.

I'm moving this back to Untriaged, because it's unclear who the subject-matter experts are (aka: who owns WebView). I don't even know the right component label for webview-in-Chrome, but wjmaclea@ may know.

[Comment 11](#) by rsleevi@chromium.org on Fri, Sep 9, 2016, 6:59 PM EDT Project Member

**Cc:** mknowles@chromium.org

[Comment 12](#) by f...@chromium.org on Mon, Sep 12, 2016, 3:37 PM EDT Project Member

**Status:** Assigned (was: Untriaged)  
**Owner:** fsam...@chromium.org

fsamuel, are you still working on WebView? If so, could you help handle or triage this bug with how WV is interacting with //net?

[Comment 13](#) by wjmaclea@chromium.org on Mon, Sep 12, 2016, 3:46 PM EDT Project Member

**Owner:** wjmaclea@chromium.org  
**Cc:** fsam...@chromium.org

I'll take a look ...

[Comment 14](#) by elawrence@chromium.org on Wed, Sep 21, 2016, 1:42 AM EDT Project Member

589150 asks for a WebView API to allow Apps to ignore HTTPS errors programmatically.

[Comment 15](#) by lgar...@chromium.org on Tue, Nov 22, 2016, 6:53 PM EST Project Member

**Components:** -Security>UX UI>Browser>Interstitials

[Comment 16](#) by est...@chromium.org on Fri, Nov 10, 2017, 2:04 PM EST Project Member

**Labels:** Hotlist-EnamelAndFriendsFixIt

[Comment 17](#) by est...@chromium.org on Sun, Feb 18, 2018, 12:45 PM EST Project Member

**Labels:** -Hotlist-EnamelAndFriendsFixIt

[Comment 18](#) by mmoroz@chromium.org on Tue, Apr 30, 2019, 1:46 AM EDT Project Member

**Labels:** M-76

Comment 19 by [sheriffbot@chromium.org](#) on Wed, Sep 11, 2019, 9:08 AM EDT Project Member

Labels: -M-76 M-77 Target-77

Comment 20 by [sheriffbot@chromium.org](#) on Wed, Oct 23, 2019, 9:18 AM EDT Project Member

Labels: -M-77 Target-78 M-78

Comment 21 by [sheriffbot@chromium.org](#) on Wed, Dec 11, 2019, 9:19 AM EST Project Member

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

Comment 22 by [est...@chromium.org](#) on Mon, Dec 16, 2019, 2:06 PM EST Project Member

Cc: [davidben@chromium.org](#)

Comment 23 by [est...@chromium.org](#) on Mon, Dec 16, 2019, 6:44 PM EST Project Member

Owner: [est...@chromium.org](#)

Taking a look at this old bug... Looks like the underlying problem is that ChromeSSLHostStateDelegate remembers certificate exceptions per-profile. The net-stack state seems to be isolated as expected (different socket pools for the app and the main browser), but clicking through a cert error in the app gets stored in ChromeSSLHostStateDelegate state that is associated with the profile and notably not segregate by StoragePartition.

I'm not totally sure how to fix this. One possibility might be to key the certificate exceptions by StoragePartition path or some such... Another option might be to move the SSLHostStateDelegate into StoragePartition.

Comment 24 by [est...@chromium.org](#) on Tue, Dec 17, 2019, 12:27 PM EST Project Member

Upon further reflection, keying off StoragePartition is probably not the way to go here. That's too fine-grained, as we generally want certificate error clickthroughs to allow loading resources from that host in a third-party context. I'm investigating another solution which would be to separate clickthroughs in a <webview> from the state for normal web browsing. That feels a little hacky/special-casey though; I'm worried there might be other cases where keying the state on the Profile is too coarse-grained...

Comment 25 by [rsleevi@chromium.org](#) on Tue, Dec 17, 2019, 12:38 PM EST Project Member

estark: StoragePartition would be associated with profiles; NetworkIsolationKey separates the third-party context. Wouldn't having <webview> be isolated from the hosting Chrome App/Chrome Profile be the right thing?

Comment 26 by [bugdroid](#) on Thu, Dec 19, 2019, 7:08 PM EST Project Member

The following revision refers to this bug:

<https://chromium.googlesource.com/chromium/src.git/+05b0dc3a708df2b3e5758fa509163d29fed02d46>

commit [05b0dc3a708df2b3e5758fa509163d29fed02d46](#)

Author: Emily Stark <[estark@google.com](#)>

Date: Fri Dec 20 00:07:34 2019

Isolate cert decisions for non-default storage partition

Currently, all cert error decisions (i.e., when a user clicks through a certificate error) are stored in ContentSettings, associated with a Profile. This means that if a user clicks through a certificate error in a <webview> in a Chrome App, that decisions propagates to normal browsing. Persisting decisions within a <webview> is undesirable on its own (because there's no UI to remind the user that they've done so and to allow them to revoke the decision), and it's especially undesirable for that decision to affect normal browsing. Therefore, this CL isolates cert error decisions by storage partition. Decisions made for the default storage partition are remembered in the normal way (ContentSettings for the Profile); decisions for other storage partitions are remembered in memory only.

[Bug=638479](#)

Change-Id: If1cca181c80f8d07f5411fbb0d3707cf3755c5a2

Reviewed-on: <https://chromium-review.googlesource.com/c/chromium/src/+1974698>

Reviewed-by: Mustafa Emre Acer <[meacer@chromium.org](#)>

Reviewed-by: Bo <[bolu@chromium.org](#)>

Reviewed-by: Alex Moshchuk <[alexmos@chromium.org](#)>

Commit-Queue: Emily Stark <[estark@chromium.org](#)>

Cr-Commit-Position: refs/heads/master@{#726607}

[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/android\\_webview/browser/aw\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/android_webview/browser/aw_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/android\\_webview/browser/aw\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/android_webview/browser/aw_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.cc](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.cc)  
[modify] [https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome\\_ssl\\_host\\_state\\_delegate.h](https://crrev.com/05b0dc3a708df2b3e5758fa509163d29fed02d46/chrome/browser/ssl/chrome_ssl_host_state_delegate.h)  
[modify]

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 31](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Jan 9, 2020, 11:59 AM EST Project Member  
Congrats! The Panel decided to reward \$500 for this report!

[Comment 32](#) by [natashapabrai@google.com](mailto:natashapabrai@google.com) on Thu, Jan 9, 2020, 12:22 PM EST Project Member  
**Labels:** -reward-unpaid reward-inprocess

[Comment 33](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, Mar 13, 2020, 1:44 PM EDT Project Member  
**Labels:** Release-0-M81

[Comment 34](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Fri, Mar 13, 2020, 2:31 PM EDT Project Member  
**Labels:** CVE-2020-6437 CVE\_description-missing

[Comment 35](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Fri, Mar 13, 2020, 3:00 PM EDT Project Member  
**Labels:** OS-Android OS-Chrome OS-Fuchsia OS-Mac OS-Windows

[Comment 36](#) by [sheriffbot](#) on Fri, Mar 27, 2020, 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 37](#) by [adetaylor@chromium.org](mailto:adetaylor@chromium.org) on Tue, Apr 14, 2020, 3:14 PM EDT Project Member  
**Labels:** -CVE\_description-missing CVE\_description-submitted

[Comment 38](#) by [adetaylor@google.com](mailto:adetaylor@google.com) on Thu, Sep 3, 2020, 11:38 AM EDT Project Member  
**Labels:** -reward-inprocess reward-decline