Starred by 5 users

Owner:	jsaul@google.com
CC:	nburris@chromium.org amyressler@google.com adetaylor@chromium.org cfroussios@chromium.org vishwasuppoor@chromium.org battre@chromium.org schwering@chromium.org maxlg@chromium.org koer...@chromium.org siyua@chromium.org adetaylor@google.com manasverma@google.com schwering@google.com armalhotra@google.com sujiezhu@google.com vidhanj@google.com koerber@google.com jsaul@google.com mlerman@chromium.org
Status:	Fixed *(Closed)*
Components:	UI>Browser>Autofill
Modified:	Oct 14, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Mac
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
reward-inprocess
Via-Wizard-Security
reward-20000
CVE_description-submitted
M-91
Target-91

Issue 1214234: Security: Heap-use-after-free in CreditCardAccessManager::FetchCreditCard

Reported by merc....@gmail.com on Fri, May 28, 2021, 6:29 AM EDT

Code

UserAgent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.77 Safari/537.36

Steps to reproduce the problem:
Note that this bug is available on devices with Touch/Face ID, Windows Hello, Android fingerprint, etc.
I use Mac for example(video1)
1. open chrome, login in your google account and add a credit card to you google account(after added you will see the card in your chrome:/setting => payment method)
2. open Touch ID in chrome://settings => payment method
2. start a https server at the folder of poc.html and credit.html and navigate to https://localhost/poc.html
3. click the first input field, it will show a popup with your credit card info, then click the credit card immediately(I set the timeout to 1s).
4. crash occurs

What is the expected behavior?

What went wrong?
In function CreditCardAccessManager::FetchCreditCard

```
347  if (should_wait_to_authenticate) {
348    card_selected_without_unmask_details_timestamp_ =
349        AutofillTickClock::NowTicks();
350
351    // Wait for |ready_to_start_authentication_| to be signaled by
352    // OnDidGetUnmaskDetails() or until timeout before calling Authenticate().
353    auto task_runner = base::ThreadPool::CreateTaskRunner({base::MayBlock()});
354    cancelable_authenticate_task_tracker_.PostTaskAndReplyWithResult( // [1] if `should_wait_to_authenticate` is true, `cancelable_authenticate_task_tracker_` will
posttask and will not cancel it even if `this` is freed.
355        task_runner.get(), FROM_HERE,
356        base::BindOnce(&WaitForEvent, &ready_to_start_authentication_),
357        base::BindOnce(&CreditCardAccessManager::Authenticate,
358                       weak_ptr_factory_.GetWeakPtr()));
359  } else {
360    Authenticate(get_unmask_details_returned);
361  }
```

After we posttask, if we delete `this`(CreditCardAccessManager) by remove the frame, the task will still alive and will called after timeout, which will use freed memory in `this`
=> UAF.
Because that the release chrome is not built with ASAN so there will be a check fail caused by UAF on MAC.

Note that there are two restrictions at line 302 and line 347
The first one is that the card you choose must be a MASKED_SERVER_CARD, therefore we need to add a credit card in your google account.

```
302   if (card->record_type() != CreditCard::MASKED_SERVER_CARD) { // the credit card you choose need to be a MASKED_SERVER_CARD
303     accessor->OnCreditCardFetched(/*did_succeed=*/true, card);
304 #if !defined(OS_IOS)
```

```
305     if (should_log_latency_metrics) {
306       AutofillMetrics::LogUserPerceivedLatencyOnCardSelection(
307           AutofillMetrics::PreflightCallEvent::kDidNotChooseMaskedCard,
308           GetOrCreateFIDOAuthenticator()->IsUserOptedIn());
309     }
310 #endif
311     return;
312   }
```

The second one is that this device must support face ID/Touch ID and so on, so we need to turn on Touch ID.

[1]
https://source.chromium.org/chromium/chromium/src/+/main:components/autofill/core/browser/payments/credit_card_access_manager.cc;drc=09e515fe7ee4d7840b15ac23edb9bbc160686fb3;l=354

==========
Chromium can not login to google account since 2021/01 (https://blog.chromium.org/2021/01/limiting-private-api-availability-in.html), therefore if you want to get a ASAN log you need to patch the chromium. Apply the patch to chrimium(which will ignore the mentioned two restrictions) and :

1. open patched chromium
2. add any credit card locally in chrome://setting => payment method
3. start a https server at the folder of poc.html and credit.html and navigator to https://localhost/poc.html
4. click the first input field, it will show a popup with your credit card info, then click the credit card immediately(timeout 1s).
5. ASAN log shows up

PS: I test chromium-886230 on Linux and use gdb to patch it for convenience, see the video2.

Did this work before? N/A

Chrome version: 91.0.4472.77 Channel: stable
OS Version:
Flash Version:

asan.txt
35.0 KB View Download

credit.html
571 bytes View Download

poc.html
536 bytes View Download

patch
1.8 KB View Download

Comment 1 by sheriffbot on Fri, May 28, 2021, 6:30 AM EDT
Labels: external_security_report

Comment 2 by merc....@gmail.com on Fri, May 28, 2021, 6:33 AM EDT
It seems that attachments can not exceed 10M, I will upload the video later.

Comment 3 by adetaylor@google.com on Fri, May 28, 2021, 12:45 PM EDT
Owner: maxlg@chromium.org
Cc: nburris@chromium.org manasverma@google.com
Labels: Security_Severity-High Security_Impact-Stable OS-Mac
Components: UI>Browser>Autofill Blink>Payments
Security sheriff here: I'm not going to attempt to reproduce this one due to the various hoops involved. This reporter has a consistent track record of finding UaFs so I'm confident it will turn out to be real!

As a browser process UaF this would be critical severity, but given the need for UI interaction I am going to downgrade it to High.

Comment 4 by sheriffbot on Fri, May 28, 2021, 12:47 PM EDT
Labels: M-91 Target-91
Setting milestone and target because of Security_Impact=Stable and high severity.

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

Comment 5 by merc....@gmail.com on Fri, May 28, 2021, 12:57 PM EDT

video1.mov
3.4 MB View Download

Comment 6 Deleted

Comment 7 by sheriffbot on Fri, May 28, 2021, 1:28 PM EDT
Labels: -Pri-2 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 8 by maxlg@chromium.org on Fri, May 28, 2021, 1:45 PM EDT

Owner: manasverma@google.com
Cc: maxlg@chromium.org

Assigning to manasverma@ because it's in Autofill codebase.

Comment 9 by sheriffbot on Fri, May 28, 2021, 2:37 PM EDT

Status: Assigned (was: Unconfirmed)

Comment 10 Deleted

Comment 11 by maxlg@chromium.org on Mon, May 31, 2021, 9:50 AM EDT

Cc: armalhotra@google.com

CC armalhotra@

Comment 12 by adetaylor@google.com on Tue, Jun 1, 2021, 8:05 PM EDT

Labels: FoundIn-91

Comment 13 by sheriffbot on Fri, Jun 11, 2021, 12:21 PM EDT

manasverma: 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 14 by maxlg@chromium.org on Fri, Jun 11, 2021, 12:48 PM EDT

Cc: siyua@chromium.org

siyua@ for triaging.

Comment 15 by merc....@gmail.com on Tue, Jun 22, 2021, 2:25 AM EDT

any update?

Comment 16 by maxlg@chromium.org on Tue, Jun 22, 2021, 9:14 AM EDT

Cc: kolos@chromium.org koer...@chromiun.org cfroussios@chromium.org

+more Chrome Autofill owners.

Comment 17 by maxlg@chromium.org on Tue, Jun 22, 2021, 9:17 AM EDT

Cc: schwering@chromium.org

schwering

Comment 18 by kolos@chromium.org on Tue, Jun 22, 2021, 9:54 AM EDT

Cc: -kolos@chromium.org

Comment 19 by maxlg@chromium.org on Tue, Jun 22, 2021, 10:14 AM EDT

Cc: jsaul@google.com

+jsaul@ as an owner of credit_card_access_manager.cc for visibility.

Comment 20 by jsaul@google.com on Tue, Jun 22, 2021, 8:27 PM EDT

Owner: jsaul@google.com

Thanks for the CC, and thanks for the report and attachments! Manas has been OOO since May 27th so this fell through the cracks just at the wrong time. I'm also coming off OOO last week so I'm still in catchup mode, but I'll try to take a look at this soon now that I'm aware of it.

Comment 21 by jsaul@google.com on Thu, Jun 24, 2021, 8:55 PM EDT

I was able to get a few minutes to take a look at this today, so I can share what I have so far. First off, I've temporarily created a version of merc.ouc@'s test page on our team's test site here, so feel free to give it a look:
https://1624581353-dot-dump-truck.appspot.com/crbug/test.html
The reproduction instructions are:
1) Have a card in pay.google.com
2) Have that card enrolled with Touch ID (you can do this by using it a couple times on https://dump-truck.appspot.com/usecase-cc/cc.html to get the appropriate prompt and opt-in event)
3) On the test page, with Touch ID now default, click into the form's first field and select the credit card within 1 second
4) After 1 second, the iframe is destroyed

However, when I try to reproduce the issue myself on Mac, I don't get a crash. Instead, it seems to correctly immediately abort the Touch ID request and falls back to a CVC auth. (The CVC auth never completes either, but it also doesn't crash.) I've attached a video recording of my tests in Chrome Canary M93, but my Chrome Stable M91 exhibits the same behavior. I suppose that means I have two questions:

1) Is there anything wrong with my setup steps such that my browser isn't crashing? The opening post mentioned "release Chrome" but does that refer to a release version of a local build and Chrome Canary is insufficient?

2) Cancelling a posted task isn't something I'm familiar with; does anyone have a good contact suggestion for who I should talk to? Is it sufficient to find a way to cancel the task in CreditCardAccessManager's destructor, or is that not an option?

Thanks!
Jared

Screen Recording 2021-06-24 at 5.41.16 PM.mov
3.0 MB View Download

Comment 22 by merc....@gmail.com on Thu, Jun 24, 2021, 10:11 PM EDT

Hi Jared, sorry for bothering your holiday.
It seems that your stpes is right and maybe you could try to shorten the time to destroy the iframe
I also test with https://1624581353-dot-dump-truck.appspot.com/crbug/test.html and the crash still occurs.
The version is 91.0.4472.114 arm64 (mac with M1 chip)

Comment 23 by merc....@gmail.com on Fri, Jun 25, 2021, 4:59 AM EDT

If you still can not repro that, maybe you can apply the patch and compile chrome, I just test it with commit 563320a900948d69ca5a65df58f9eadc385447ef on ubuntu, and repro successfully.

Comment 24 by jsaul@google.com on Fri, Jun 25, 2021, 5:29 PM EDT

No worries about the holiday bit, I'm just sorry I can't give this more focus at the moment because we have a lot going on. I can try it with a compiled build when I next get a chance. (I'm also gone for another week in 6 more days so this will likely repeat next month...)

In the meantime, do you know of any sites in the wild where this issue occurs? I assume that removing an iFrame immediately upon interacting with it is an extremely rare use case, which is why we haven't heard of this happening before. I agree this is an issue that should be fixed, I'm just trying to gauge the urgency.

I'll also reach out to a couple of my colleagues on a suggested fix for a deleted posttask.

Comment 25 by merc....@gmail.com on Fri, Jun 25, 2021, 9:42 PM EDT

I don't find any sites in wild with this issue...

Comment 26 by jsaul@google.com on Wed, Jun 30, 2021, 1:00 PM EDT

Cc: battre@chromium.org

Comment 27 by battre@chromium.org on Wed, Jun 30, 2021, 5:35 PM EDT

I think that the fix is as simple as changing the destructor of CreditCardAccessManager to this:

```
CreditCardAccessManager::~CreditCardAccessManager() {
  // Ensure that we are not waiting when the WaitableEvent is destroyed.
  ready_to_start_authentication_.Signal();
}
```

Unfortunately, I cannot get my local MacOS build to offer me TouchID, yet. - Even though the official Dev/Canary builds do.

@merc.ouc could you please give it a try and confirm that this fixes the problem?

Comment 28 by merc....@gmail.com on Thu, Jul 1, 2021, 2:56 AM EDT

I only have a local ubuntu built environment, and I apply battre@'s patch and my patch in comment1. Unfortunately, the uaf still occurs.

Comment 29 by battre@chromium.org on Thu, Jul 1, 2021, 5:59 PM EDT

Cc: koerber@google.com schwering@google.com

I have uploaded a patch here: https://chromium-review.googlesource.com/c/chromium/src/+/3001123

Turned out to be much more complex than expected, because ready_to_start_authentication_ could be used after the deallocation and I did not find a way to cancel the task in a trustworthy way.

Manas and Jared, I hope that you have a working setup to test the biometric reauth. Please do. I learned that I need to take a gazillion hoops to build a binary that get access to the biometric sensors on a mac.

I was able to reproduce the crash with "patch" from the initial commend and the crash does not happen anymore.

I am pretty confident that the crash is fixed. But I would like to seek validation that I have not broken anything as I am not super familiar with the CreditCardAccessManager.

Comment 30 by jsaul@google.com on Thu, Jul 1, 2021, 8:00 PM EDT

Thanks Dominic, I really appreciate your expertise. The CL looks great, AFAICT.

Unfortunately I *don't* have a working setup to test the biometric reauth. I believe Manas did, but he's unavailable now. I'm creating a ToT build on my Mac for a different issue but I doubt I'll have it ready for testing by tomorrow, and I'm OOO next week for the holiday. :(

I'd be happy to help test correctness on Canary in the interim, but given that my Canary/Stable builds don't crash (#c29) I think I would only be able to test correctness of the happy path.

Comment 31 by Git Watcher on Fri, Jul 2, 2021, 1:37 PM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/48cf01e4039fecbe119d8223d1f6072aaf44f258

commit 48cf01e4039fecbe119d8223d1f6072aaf44f258
Author: Dominic Battre <battre@chromium.org>
Date: Fri Jul 02 17:36:12 2021

Replace first of two WaitableEvents in CreditCardAccessManager

~~Bug: 1214234~~
Change-Id: I38171be7b38982f25abfbb3dff7a41f19a167764
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3001123
Reviewed-by: Jared Saul <jsaul@google.com>
Commit-Queue: Dominic Battré <battre@chromium.org>

Cr-Commit-Position: refs/heads/master@{#898237}

[modify] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/BUILD.gn
[modify] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/credit_card_access_manager.cc
[modify] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/credit_card_access_manager.h
[modify] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/credit_card_access_manager_unittest.cc
[add] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/wait_for_signal_or_timeout.cc
[add] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/wait_for_signal_or_timeout.h
[add] https://crrev.com/48cf01e4039fecbe119d8223d1f6072aaf44f258/components/autofill/core/browser/payments/wait_for_signal_or_timeout_unittest.cc

Comment 32 by battre@chromium.org on Tue, Jul 6, 2021, 8:04 AM EDT

Cc: vidhanj@google.com

Comment 33 by battre@chromium.org on Tue, Jul 6, 2021, 8:34 AM EDT

Status: Fixed (was: Assigned)

Comment 34 by sheriffbot on Tue, Jul 6, 2021, 12:42 PM EDT

Labels: reward-topanel

Comment 35 by sheriffbot on Tue, Jul 6, 2021, 2:02 PM EDT

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

Comment 36 by sheriffbot on Tue, Jul 6, 2021, 2:23 PM EDT

Labels: Merge-Request-92 Merge-Request-91

Requesting merge to stable M91 because latest trunk commit (898237) appears to be after stable branch point (870763).

Requesting merge to beta M92 because latest trunk commit (898237) appears to be after beta branch point (885287).

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

Comment 37 by sheriffbot on Tue, Jul 6, 2021, 2:28 PM EDT

Labels: -Merge-Request-92 Merge-Review-92 Hotlist-Merge-Review

This bug requires manual review: We are only 13 days from stable.
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/+/main/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: govind@(Android), benmason@(iOS), dgagnon@(ChromeOS), srinivassista@(Desktop)

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

Comment 38 by battre@chromium.org on Wed, Jul 7, 2021, 10:33 AM EDT

Cc: adetaylor@chromium.org

1. Deferring to adetaylor@ for an assessment of criticality
2. https://chromium-review.googlesource.com/c/chromium/src/+/3001123
3. Yes
4. Deferring to adetaylor@
5. Security vulnerability
6. no
7. n/a

@jsaul, @armalhotra: On Android I could not get biometric credit card unlocking to work (neither on stable nor on Dev/Canary). On MacOS I could get the unlocking via OS Password to work but not via the finger print scanner in the device.

Comment 39 by adetaylor@google.com on Wed, Jul 7, 2021, 11:37 AM EDT

Labels: -Merge-Review-92 Merge-Approved-92

Approving merge to M92, please merge to branch 4515.

Comment 40 by jsaul@google.com on Wed, Jul 7, 2021, 2:54 PM EDT

I successfully tested biometric auth in Mac Canary 93.0.4563.0 (before the fix) and 93.0.4568.0 (after the fix). I'm asking my team to test on Clank as well.

Comment 41 by Git Watcher on Wed, Jul 7, 2021, 4:04 PM EDT

Labels: -merge-approved-92 merge-merged-4515 merge-merged-92

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/24293de1553b49f74d0846d2c93fde07eec2d151

commit 24293de1553b49f74d0846d2c93fde07eec2d151
Author: Dominic Battre <battre@chromium.org>
Date: Wed Jul 07 20:02:45 2021

Replace first of two WaitableEvents in CreditCardAccessManager

(cherry picked from commit 48cf01e4039fecbe119d8223d1f6072aaf44f258)

~~Bug: 1214234~~
Change-Id: I38171be7b38982f25abfbb3dff7a41f19a167764
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3001123
Reviewed-by: Jared Saul <jsaul@google.com>
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#898237}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3011066
Reviewed-by: Dominic Battré <battre@chromium.org>
Reviewed-by: Prudhvi Kumar Bommana <pbommana@google.com>
Owners-Override: Prudhvi Kumar Bommana <pbommana@google.com>
Cr-Commit-Position: refs/branch-heads/4515@{#1366}

Cr-Branched-From: 488fc70865ddaa05324ac00a54a6eb783b4bc41c-refs/heads/master@{#885287}

[modify] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/BUILD.gn
[modify] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/credit_card_access_manager.cc
[modify] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/credit_card_access_manager.h
[modify] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/credit_card_access_manager_unittest.cc
[add] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/wait_for_signal_or_timeout.cc
[add] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/wait_for_signal_or_timeout.h
[add] https://crrev.com/24293de1553b49f74d0846d2c93fde07eec2d151/components/autofill/core/browser/payments/wait_for_signal_or_timeout_unittest.cc

Comment 42 by siyua@chromium.org on Wed, Jul 7, 2021, 7:00 PM EDT

Cc: sujiezhu@google.com vishwasuppoor@chromium.org

Comment 43 by rouslan@chromium.org on Tue, Jul 13, 2021, 10:49 AM EDT

Components: -Blink>Payments

Not related to PaymentRequest API.

Comment 44 by amyressler@chromium.org on Mon, Jul 19, 2021, 3:09 PM EDT

Labels: Release-0-M92

Comment 45 by amyressler@google.com on Mon, Jul 19, 2021, 7:15 PM EDT

Labels: CVE-2021-30572 CVE_description-missing

Comment 46 by amyressler@google.com on Thu, Jul 22, 2021, 1:05 PM EDT

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 47 by amyressler@google.com on Thu, Jul 22, 2021, 1:15 PM EDT

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

Comment 48 by merc....@gmail.com on Thu, Jul 22, 2021, 10:31 PM EDT

Thank you!

Comment 49 by amyressler@google.com on Fri, Jul 23, 2021, 1:04 PM EDT

Labels: -Merge-Request-91 Merge-Approved-91

Merge approved to M91, which is now the Extended Stable release branch; please merge to branch 4472 at your earliest convenience. Thank you!

Comment 50 by amyressler@google.com on Fri, Jul 23, 2021, 6:18 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 51 by rzanoni@google.com on Tue, Jul 27, 2021, 9:05 AM EDT

Labels: LTS-Security-90 LTS-Merge-Request-90

Comment 52 by sheriffbot on Tue, Jul 27, 2021, 12:14 PM EDT

Cc: adetaylor@google.com amyressler@google.com

This issue has been approved for a merge. Please merge the fix to any appropriate branches as soon as possible!

If all merges have been completed, please remove any remaining Merge-Approved labels from this issue.

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 53 by Git Watcher on Tue, Jul 27, 2021, 4:10 PM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/84b97683080071a1d526b7c5d3727eb9db5681f3

commit 84b97683080071a1d526b7c5d3727eb9db5681f3
Author: Dominic Battre <battre@chromium.org>
Date: Tue Jul 27 20:09:16 2021

[M91] Replace first of two WaitableEvents in CreditCardAccessManager

(cherry picked from commit 48cf01e4039fecbe119d8223d1f6072aaf44f258)

~~Bug: 1214234~~
Change-Id: I38171be7b38982f25abfbb3dff7a41f19a167764
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3001123
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#898237}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3055959
Auto-Submit: Dominic Battré <battre@chromium.org>
Commit-Queue: Jared Saul <jsaul@google.com>
Reviewed-by: Jared Saul <jsaul@google.com>
Cr-Commit-Position: refs/branch-heads/4472@{#1580}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/BUILD.gn
[modify] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/credit_card_access_manager.cc
[modify] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/credit_card_access_manager.h
[modify] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/credit_card_access_manager_unittest.cc
[add] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/wait_for_signal_or_timeout.cc
[add] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/wait_for_signal_or_timeout.h
[add] https://crrev.com/84b97683080071a1d526b7c5d3727eb9db5681f3/components/autofill/core/browser/payments/wait_for_signal_or_timeout_unittest.cc

Comment 54 by rzanoni@google.com on Wed, Jul 28, 2021, 3:14 AM EDT

Labels: LTS-Size-Normal LTS-Complexity-Minimal

Comment 55 by gianluca@google.com on Wed, Jul 28, 2021, 4:39 AM EDT

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

Comment 56 by Git Watcher on Wed, Jul 28, 2021, 5:19 AM EDT

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

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/090bb29f567ec34aeff85878f92025b9fd976bba

commit 090bb29f567ec34aeff85878f92025b9fd976bba
Author: Dominic Battre <battre@chromium.org>
Date: Wed Jul 28 09:18:06 2021

[M90-LTS] Replace first of two WaitableEvents in CreditCardAccessManager

(cherry picked from commit 48cf01e4039fecbe119d8223d1f6072aaf44f258)

~~Bug: 1214234~~
Change-Id: I38171be7b38982f25abfbb3dff7a41f19a167764
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3001123
Commit-Queue: Dominic Battré <battre@chromium.org>
Cr-Original-Commit-Position: refs/heads/master@{#898237}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3055362
Reviewed-by: Dominic Battré <battre@chromium.org>
Reviewed-by: Jana Grill <janagrill@google.com>
Commit-Queue: Roger Felipe Zanoni da Silva <rzanoni@google.com>
Cr-Commit-Position: refs/branch-heads/4430@{#1544}
Cr-Branched-From: e5ce7dc4f7518237b3d9bb93cccca35d25216cbe-refs/heads/master@{#857950}

[modify] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/BUILD.gn
[modify] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/credit_card_access_manager.cc
[modify] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/credit_card_access_manager.h
[modify] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/credit_card_access_manager_unittest.cc
[add] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/wait_for_signal_or_timeout.cc
[add] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/wait_for_signal_or_timeout.h
[add] https://crrev.com/090bb29f567ec34aeff85878f92025b9fd976bba/components/autofill/core/browser/payments/wait_for_signal_or_timeout_unittest.cc

Comment 57 by rzanoni@google.com on Wed, Jul 28, 2021, 5:45 AM EDT

Labels: -LTS-Merge-Approved-90 LTS-Merged-90

Comment 58 by amyressler@google.com on Tue, Aug 3, 2021, 3:41 PM EDT

Labels: -CVE_description-missing CVE_description-submitted

Comment 59 by sheriffbot on Thu, Oct 14, 2021, 1:29 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