Starred by 4 users

Owner:	martinkr@google.com
CC:	manasverma@google.com nsatr...@chromium.org kenrb@chromium.org martinkr@google.com battre@chromium.org agl@chromium.org mlerman@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebAuthentication UI>Browser>Autofill>UI
Modified:	Aug 19, 2021
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Android
Pri:	1
Type:	Bug-Security

Hotlist-Merge-Review
Security_Impact-Stable
Security_Severity-High
allpublic
CVE_description-submitted
M-90
Target-90
LTS-Security-86
LTS-Security-NotApplicable-86
merge-merged-4472
merge-merged-91
LTS-Security-90
LTS-Security-NotApplicable-90
Release-0-M91
CVE-2021-30528

Issue 1206329: UAF in InternalAuthenticatorAndroid::InvokeIsUserVerifyingPlatformAuthenticatorAvailableResponse

Reported by m...@semmle.com on Thu, May 6, 2021, 12:53 PM EDT

Code

VULNERABILITY DETAILS
When fetching credit card details for autofill, |IsUserVerifyingPlatformAuthenticatorAvailable| will be called [1]. On Android, this will call the corresponding method of the Java class |InternalAuthenticator| [2]. This method then stores |mNativeInternalAuthenticatorAndroid| in a callback [3] as a Java lambda. Although |mNativeInternalAuthenticatorAndroid| owns a reference to this |InternalAuthenticator| [4] and will normally destroy this |InternalAuthenticator| when it is destroyed, by storing |mNativeInternalAuthenticatorAndroid| in a Java lambda, the lambda callback will also hold a shared reference to the |InternalAuthenticator|. This means even if the |mNativeInternalAuthenticator| is destroyed, the Java lambda can still be keeping |InternalAuthenticator| alive, while |mNativeInternalAuthenticator| will now point to a free'd object. When the callback is finally invoked, a UAF will happen. [5] As the lifetime of |mNativeInternalAuthenticator| is bound to the |RenderFrameHost| that transitively owns it, it can be freed by destroying an iframe that holds it from the renderer before the Java callback is invoked.

VERSION
Tested on Pixel 3a firmware version RQ2A.210405.005, Android 11
Chromium stable build 90.0.4430.91

REPRODUCTION CASE
This issue requires the user to have already saved a credit card in their Google Account (Probably using this feature [5]), not just on the phone. To emulate this for testing, apply the |browser.patch|, which will remove the check for server card in |PrepareToFetchCreditCard|, so that locally stored card will also trigger the bug.

```
void CreditCardAccessManager::PrepareToFetchCreditCard() {
#if !defined(OS_IOS)
  // No need to fetch details if there are no server cards.
  if (!ServerCardsAvailable())
    return;
```

It also removes the |IsFormNonSecure| check in |autofill_manager.cc| to make local testing easier (This test should pass for any https website, but not with self signed certificate) After that, add a local card in the phone in settings > Payment methods so that Chrome will be able to fetch a card. For testing, the card number 4111 1111 1111 1111 can be used (which will pass as a valid card number), the other fields can be arbitrary. The patch is based on version 90.0.4430.91 and there are some changes in file names in the master branch, so it may not apply cleanly to the master branch.

These steps will emulate having a card stores remotely, which is necessary to trigger the bug.

After that, apply the |authn.patch| to emulate a compromised renderer. The bug can probably triggered without a compromised renderer as all the patch does is to trigger a credit card prefetch, which would happen when user tries to fill in a form with credit card field. A compromised renderer removes the need for user gesture.

Then put the files |trigger.html|, |trigger2.html| and |trigger_jam.html| in the same directory and open |trigger2.html| with Chrome on an Android device:

$ out/Release/bin/chrome_public_apk run http://localhost:8000/trigger2.html

If successful, Chrome would crash with a log similar to the attached |crash.log|. It should trigger reliably, although may require a few refreshes and may need a real phone with production image to trigger.

Thank you very much for your help and please let me know if there is anything that I can help.

1. https://source.chromium.org/chromium/chromium/src/+/f95d0eb0ad8e7671f2a8171ff96cad06973423cb:components/autofill/core/browser/payments/credit_card_fido_authenti

cator.cc;l=148;bpv=0;bpt=1
2.
https://source.chromium.org/chromium/chromium/src/+/f95d0eb0ad8e7671f2a8171ff96cad06973423cb:chrome/browser/autofill/android/internal_authenticator_android.cc;l=94;drc=c3fe176a27dcad95b576fa233c63d7238b138af4;bpv=1;bpt=1
3.
https://source.chromium.org/chromium/chromium/src/+/f95d0eb0ad8e7671f2a8171ff96cad06973423cb:chrome/android/java/src/org/chromium/chrome/browser/autofill/InternalAuthenticator.java;l=98;bpv=1;bpt=1
4.
https://source.chromium.org/chromium/chromium/src/+/f95d0eb0ad8e7671f2a8171ff96cad06973423cb:chrome/browser/autofill/android/internal_authenticator_android.cc;l=34;drc=c3fe176a27dcad95b576fa233c63d7238b138af4;bpv=1;bpt=1
5.
https://source.chromium.org/chromium/chromium/src/+/f95d0eb0ad8e7671f2a8171ff96cad06973423cb:chrome/browser/autofill/android/internal_authenticator_android.cc;l=152;drc=c3fe176a27dcad95b576fa233c63d7238b138af4;bpv=1;bpt=1
6. https://blog.chromium.org/2019/07/easier-payments-with-chrome.html?m=1

CREDIT INFORMATION
Reporter credit: Man Yue Mo of GitHub Security Lab

trigger.html
178 bytes View Download

trigger2.html
726 bytes View Download

trigger_jam.html
196 bytes View Download

crash_log.txt
13.0 KB View Download

authn.patch
2.9 KB View Download

browser.patch
1.3 KB View Download

Comment 1 by rsleevi@chromium.org on Thu, May 6, 2021, 2:42 PM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: agl@chromium.org
Cc: manasverma@google.com
Labels: Security_Impact-Stable Security_Severity-High OS-Android Pri-2
Components: UI>Browser>Autofill>UI Blink>WebAuthentication

Adam: I saw you recently tackled a (different) UAF risk in https://chromium-review.googlesource.com/c/chromium/src/+/2773782 several weeks ago - would you be good to peep this? I haven't repro'd for lack of a Android device here, but I'm guessing you might already have an environment spun up, and the code trace looks right. Is this a risk for the other lambda-binding of |mNativeInternalAuthenticatorAndroid| ?

CC'ing manasverma@ as another active contributor in this area

Comment 2 by martinkr@google.com on Thu, May 6, 2021, 9:15 PM EDT Project Member

Status: Started (was: Assigned)
Owner: martinkr@google.com

(Taking this since I just looked at this code.)

This certainly looks right. Unfortunately I can't get those renderer changes to build. Could you tell me if you made any BUILD file changes to coax it to build with your patch?

The fix I think would be to set the Java-side mNativeInternalAuthenticatorAndroid to 0 when InternalAuthenticatorAndroid is destroyed, and check for 0 before making Java-to-Native calls.

Comment 3 by m...@semmle.com on Fri, May 7, 2021, 9:20 AM EDT

Thanks for looking into this. I've checked and I haven't made any changes to the BUILD file. The patch is based off feeb9bd (90.0.4430.91). There are some changes between this branch and the master branch. Try these patches for the master branch (74674e0). I've tested these and they should work.

renderer.patch
3.3 KB View Download

browser.patch
1.4 KB View Download

Comment 4 by sheriffbot on Fri, May 7, 2021, 12:47 PM EDT Project Member

Labels: M-90 Target-90

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 sheriffbot on Fri, May 7, 2021, 1:27 PM EDT Project Member

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 6 by Git Watcher on Tue, May 11, 2021, 12:36 PM EDT Project Member

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/2111de45d384a62deff0b85a2990f92d40102ba3

commit 2111de45d384a62deff0b85a2990f92d40102ba3
Author: Martin Kreichgauer <martinkr@google.com>
Date: Tue May 11 16:35:24 2021

Clear InternalAuthenticator's native pointer when it is destroyed

~~Bug: 1206239~~
Change-Id: I399b97b2a5162da2da289b60711913911b1df389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885427
Reviewed-by: Adam Langley <agl@chromium.org>
Reviewed-by: Colin Blundell <blundell@chromium.org>
Commit-Queue: Martin Kreichgauer <martinkr@google.com>
Cr-Commit-Position: refs/heads/master@{#881564}

[modify] https://crrev.com/2111de45d384a62deff0b85a2990f92d40102ba3/chrome/android/java/src/org/chromium/chrome/browser/autofill/InternalAuthenticator.java
[modify] https://crrev.com/2111de45d384a62deff0b85a2990f92d40102ba3/chrome/browser/autofill/android/internal_authenticator_android.cc

Comment 7 by martinkr@google.com on Tue, May 11, 2021, 2:13 PM EDT Project Member

Status: Fixed (was: Started)

Thanks for the instructions. Applying the original patches to HEAD caused some build dependency issues that I wasn't sure how to resolve, but the updated version on top of feeb9bd built fine. I managed to get a repro and could confirm that the above commit fixes the crash. Good find!

Comment 8 by sheriffbot on Tue, May 11, 2021, 2:22 PM EDT Project Member

Labels: Merge-Request-90 Merge-Request-91

Requesting merge to stable M90 because latest trunk commit (881564) appears to be after stable branch point (857950).

Requesting merge to beta M91 because latest trunk commit (881564) appears to be after beta branch point (738).

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

Comment 9 by sheriffbot on Tue, May 11, 2021, 2:23 PM EDT Project Member

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

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/+/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), marinakz@(ChromeOS), pbommana@(Desktop)

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

Comment 10 by martinkr@google.com on Tue, May 11, 2021, 2:45 PM EDT Project Member

>1. Does your merge fit within the Merge Decision Guidelines?
Yes. This is a browser process UAF.

> 2. Links to the CLs you are requesting to merge.
see #comment6

> 3. Has the change landed and been verified on ToT?
Yes

> 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?
It's a high severity security issue, so we should merge it to M90 and M91.

> 6. Is this a new feature?
> 7. If it is a new feature, is it behind a flag using finch?
Not a new feature.

Comment 11 by m...@semmle.com on Wed, May 12, 2021, 7:49 AM EDT

Thanks. I've checked against commit f04cb23 on master branch and can confirm that the patch is effective. Thanks.

Comment 12 by benmason@google.com on Wed, May 12, 2021, 10:11 AM EDT Project Member

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

CL in comment 6 approved to merge to M91, branch 4472.

Comment 13 by Git Watcher on Wed, May 12, 2021, 1:39 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/+/2efef52b891d4ae0a3ae96a94bbb9fdef212e7ed

commit 2efef52b891d4ae0a3ae96a94bbb9fdef212e7ed
Author: Martin Kreichgauer <martinkr@google.com>
Date: Wed May 12 17:38:04 2021

[M91] Clear InternalAuthenticator's native pointer when it is destroyed

(cherry picked from commit 2111de45d384a62deff0b85a2990f92d40102ba3)

~~Bug: 1206329~~
Change-Id: I399b97b2a5162da2da289b60711913911b1df389
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2885427
Reviewed-by: Adam Langley <agl@chromium.org>
Reviewed-by: Colin Blundell <blundell@chromium.org>
Commit-Queue: Martin Kreichgauer <martinkr@google.com>
Cr-Original-Commit-Position: refs/heads/master@{#881564}
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/2892421
Commit-Queue: Colin Blundell <blundell@chromium.org>
Auto-Submit: Martin Kreichgauer <martinkr@google.com>
Cr-Commit-Position: refs/branch-heads/4472@{#1000}
Cr-Branched-From: 3d60439cfb36485e76a1c5bb7f513d3721b20da1-refs/heads/master@{#870763}

[modify] https://crrev.com/2efef52b891d4ae0a3ae96a94bbb9fdef212e7ed/chrome/android/java/src/org/chromium/chrome/browser/autofill/InternalAuthenticator.java
[modify] https://crrev.com/2efef52b891d4ae0a3ae96a94bbb9fdef212e7ed/chrome/browser/autofill/android/internal_authenticator_android.cc

Comment 14 by sheriffbot on Wed, May 12, 2021, 2:02 PM EDT Project Member

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

Comment 15 by adetaylor@google.com on Fri, May 21, 2021, 3:43 PM EDT Project Member

Labels: -Merge-Request-90

Comment 16 by amyressler@chromium.org on Mon, May 24, 2021, 11:03 AM EDT Project Member

Labels: Release-0-M91

Comment 17 by amyressler@google.com on Mon, May 24, 2021, 2:18 PM EDT Project Member

Labels: CVE-2021-30528 CVE_description-missing

Comment 18 by achuith@chromium.org on Thu, May 27, 2021, 3:20 PM EDT Project Member

Labels: LTS-Security-86 LTS-Security-NotApplicable-86

Comment 19 by asumaneev@google.com on Mon, Jun 7, 2021, 2:59 PM EDT Project Member

Labels: LTS-Security-90 LTS-Security-NotApplicable-90

Marking not applicable for LTS since Android-only issue.

Comment 20 by amyressler@google.com on Mon, Jun 7, 2021, 3:27 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 21 by sheriffbot on Thu, Aug 19, 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