Starred by 3 users

Owner: vasi...@chromium.org

CC: allamkavya@chromium.org
cthomp@chromium.org
kolos@chromium.org
harrisonsean@chromium.org

Status: Fixed *(Closed)*

Components: UI>Browser>Passwords
Privacy

Modified: Jul 29, 2022

Backlog-Rank: ----

Editors: ----

EstimatedDays: ----

NextAction: ----

OS: Linux, Windows, Mac

Pri: 2

Type: Bug-Security

reward-500
Security_Severity-Low
Security_Impact-Stable
Security_Impact-None
allpublic
reward-inprocess
CVE_description-submitted
Target-97
M-97
external_security_report
FoundIn-95
FoundIn-96
FoundIn-97
TE-Verified-M98
TE-Verified-98.0.4697.0
Release-0-M97
CVE-2022-0120

Issue 1262953: Improper restriction in password saving form, while navigation from one site to another site

Reported by chakr...@gmail.com on Mon, Oct 25, 2021, 6:37 AM EDT

Code

Report description

Improper restriction in password saving form, while navigation from one site to another site

---

Bug location

Which product or website have you found a vulnerability in?

Google Chrome

Which URL have you found the vulnerability in?

No url

The problem

Please describe the technical details of the vulnerability

Password saving form is not getting closed and also holding the password when user visit to different websites.

Steps:

1.Visit the Login page of any website for example www.facebook.com/login

2.Enter the credentials

3.After entering the password there will be a key icon will get displayed on the right side of the top URL bar.

4.Click on the key icon , the password auto saving form will get displayed

5.Click on the EYE button (After clicking on the eye icon you can see the entered password)

6.Now without closing the password form , Enter a new different website URL on the same tab

6.Now without closing the password form , Enter a new different website URL on the same tab.

7.The second website will get loaded on the same tab, But the password form will remain as it is.

There should be a restriction in password form when the user try to visit the different website , Either the password field or the entire form should get cleared out.

Since there is no restriction there is chance that the credentials of one website can be leaked to other website via this improper restriction in password form of the browser.

Please briefly explain who can exploit the vulnerability, and what they gain when doing so

I compared the similar feature with Firefox browser and it seems that the Firefox handles the password form better than the chrome browser.

Please refer the attached video for reference.

The cause

What version of Chrome have you found the security issue in?

Version 94.0.4606.81 (Official Build) (arm64)

Is the security issue related to a crash?

No

Choose the type of vulnerability

Caching

Please provide your credit information

CHAKRAVARTHI (Ruler96)

Comment 1 by chrom...@appspot.gserviceaccount.com on Mon, Oct 25, 2021, 6:37 AM EDT

Labels: external_security_report

Comment 2 by chakr...@gmail.com on Mon, Oct 25, 2021, 6:58 AM EDT

POC attached in the below link

https://drive.google.com/file/d/1Z0LzlkuShOwet01gSXCHxgbsEURCbPxL/view?usp=sharing

Comment 3 by est...@chromium.org on Mon, Oct 25, 2021, 7:21 PM EDT

Labels: -Restrict-View-SecurityTeam Security_Impact-None Restrict-View-Google Type-Bug
Components: UI>Browser>Passwords Privacy

Sending over to password manager team to see if this is working as intended. This wouldn't be a security bug unless perhaps saving the password after navigating away saves the password to the wrong site. It could be that the dialog intentionally persists to give the user a chance to save their password even after navigating away.

Comment 4 Deleted

Comment 5 Deleted

Comment 6 by chakr...@gmail.com on Mon, Oct 25, 2021, 10:24 PM EDT

I tested the behaviour which you mentioned in the comment section (unless perhaps saving the password after navigating away saves the password to the wrong site).

After the navigation, it actually saving the password to the wrong site.

Comment 7 by chakr...@gmail.com on Mon, Oct 25, 2021, 10:38 PM EDT

And it is happening on a specific scenario,

Steps,

1.On the first site fill login the details and open the password dialog dialog form.

2.Now keeping the dialog open, navigate to the other sites login page

3.Now enter something in the other site login page password field (entering one letter in password field is enough)

4.Now click save button in the dialog

5.The password of first site will get save to the wrong site.

Comment 8 by allamkavya@chromium.org on Tue, Oct 26, 2021, 7:30 AM EDT

Status: Untriaged (was: Unconfirmed)
Cc: allamkavya@chromium.org
Labels: FoundIn-95 FoundIn-96 FoundIn-97 Target-97 M-97 OS-Linux OS-Mac OS-Windows Pri-2

Able to reproduce the issue on reported chrome version #94.0.4606.81 as per steps in C#0 and C#7

Reproducible on:

Canary: #97.0.4682.0

Dev: #97.0.4676.0
Beta: #96.0.4664.18
Stable: #95.0.4638.54

Stable: #95.0.4638.54

As the issue is reproducible since M81(#81.0.4044.0), considering it as non-regression issue and marking it as 'Untriaged' so that someone from respective team could take a look into it.

Thanks

1262953.webm
5.4 MB View Download

Comment 9 by chakr...@gmail.com on Wed, Oct 27, 2021, 11:07 PM EDT

Hi Team,

I think this is kind a more serious than i thought.

There is a chance that the millions of users credentials could have been exposed from one site to other site.

On my previous steps i have mentioned that after login in to first site we need to manually open the password dialog.

Actually we don't have to do that.

If we login to first site with valid credentials the password dialog automatically pops up.

Without closing the dialog if we navigate to any new site and enter credentials over there and save it.

Credentials will be saved on wrong site.

So far the credentials is not exposed to other site.

But if the users again visit the wrong site on some other day and uses the saved password.

The moment when he click on the login button with the wrong saved credentials.

He is exposing the credentials from one site to other site without his knowledge

He is exposing the credentials from one site to other site without his knowledge.

I just wanted to share my thoughts.I think the POC on comment 8 explains it all.

Please let me know about your thoughts.

Thanks,
Chakravarthi.

Comment 10 by harrisonsean@chromium.org on Thu, Oct 28, 2021, 5:16 AM EDT

Owner: vasi...@chromium.org
Cc: harrisonsean@chromium.org

sending to password manager team to traige

Comment 11 by chakr...@gmail.com on Mon, Nov 1, 2021, 5:10 AM EDT

Hi Team Any update?

As per my understanding this issue should not be disclosed to public for some period of time.

Since this issue is there in almost every version of chrome including all the Operating systems.

There is a high probability that many users might have already exposed their credentials to wrong site.

Also if we did not patch this issue quickly, there is a chance that many user may expose their credentials in future also.

Let see how this issue can be exploited from my perspective,

1.Consider an Admin of the large organisation like Facebook.
2.Surely all the big organisations will have proper logging monitoring systems, which will log all the details about invalid login attempts.
3.If the admin of the organisation is get to know about this vulnerability, they can just do the quick audit about all the invalid login attempts.
4.Also they can filter out all the invalid login attempts made form the specific user agents.
5.They can include the filter to get all the attempts from specific version.(In our case all the versions mentioned in comment 8)
6.So because of this flaw, If any user who unknowingly saved and tried to login to Facebook with wrong data.
7.They will become the victim for this vulnerability. (Without there knowledge)

There are so many organisations and who also uses this kind of logging monitoring system.

If every organisation tried to do the steps which i mentioned above, there is a high probability that millions of credentials could get exposed from one site to other site.

So far the betterment of world.

I pledge myself, Not to disclose this bug even after fixing this.

Please correct me, If i am wrong.

Looking forward for your reply.

Have a good day

Have a good day.

Thanks,
Chakravarthi.

Comment 12 by vasi...@chromium.org on Tue, Nov 2, 2021, 7:21 AM EDT

I will take care of it. We don't consider it high impact because in reality nobody does the step 4 in the original description.

Comment 13 by chakr...@gmail.com on Tue, Nov 2, 2021, 7:33 AM EDT

If you are refering the 4.Click on the key icon....

Please have a look at comment 9 also.

We don't have to click on the key icon..The password dialog automatically pops up if we login with valid credentials..

Comment 14 by chakr...@gmail.com on Tue, Nov 2, 2021, 10:24 AM EDT

I agree with you that most of the time, the users will not manually open the password dialog by using key icon.

But the above mentioned issue is happening for automatically opened dialog also.

When will the Password dialog will automatically pops up?

The password dialog form will automatically pops up, if user is logged in to the new website with valid login credentials.

Now there are only two ways that they can get rid of the password dialog in current tab.

1.Saving the valid credentials to the same site.

2.or User should manually close the dialog.

If user is not doing any of the above two steps .

Without closing the dialog, if they proceed to visit any other site and also enter any data on the password field of the other site .(Definitely they become victim for this issue)

One more thing we should consider here,

An average size of the desktop screen is 22 to 24 inches.

If users were using desktop of 24 inches, there is high chance that they might not even located the automatically popped up password dialog.

There is high chance that they might become victim for this issue.

In order to get rid of all the above mentioned issue ,

If we provide the functionality like, when user is switching from one site to other site the password dialog should clear out all the data ,

Irrespective of whether it is in open on not in open state.

or

It should not save data of one site to other site.

Please share your thoughts.

Have a good day.

Thanks,
Chakravarthi.

Comment 15 by kolos@google.com on Tue, Nov 2, 2021, 10:43 AM EDT

Status: Available (was: Untriaged)
Cc: kolos@chromium.org

This is indeed an issue.

Comment 16 by vasi...@chromium.org on Tue, Nov 2, 2021, 11:55 AM EDT

If you don't open the bubble manually but only login in on different sites then the bubble is refreshed automatically. You will always see the password from the last login page and "Save" results in the last password being saved on the correct site. It's the behavior in the current Chrome Stable 95.

Comment 17 by chakr...@gmail.com on Tue, Nov 2, 2021, 12:10 PM EDT

No it is not refreshing.

I have tested it just now on the version (Version 95.0.4638.69 (Official Build) (arm64)), it is not refreshing.

It is behaving the same way as shown in POC comment 8.

It is failing on the specific scenario which in mentioned in comment 7.

It is saving the password to wrong site, even without manually opening the bubble.

Comment 18 by vasi...@chromium.org on Tue, Nov 2, 2021, 12:23 PM EDT

1. Login with fake data on http://1.chromium-test1.appspot.com/
2. Observer the bubble.
3. Navigate and login on https://rsolomakhin.github.io/autofill/
4. Observe the new bubble with new credentials.
5. Save. The password is saved on https://rsolomakhin.github.io/autofill/

What are your reproduction steps?

Comment 19 by chakr...@gmail.com on Tue, Nov 2, 2021, 12:33 PM EDT

No login with correct data in first site.. it will automatically pop ups the data of first site.

Now without closing the bubble navigate to second site.

Give some data on the password field of the second site.

Now click on save.

It will save the data of first site to second site.

Comment 20 by chakr...@gmail.com on Tue, Nov 2, 2021, 12:45 PM EDT

Sorry if i made mistake on the above steps,

Here is the exact reproduction step,

1.Loin to any new site with valid login credentials.
2.When you login to any new site it will automatically open the bubble.
3.Now don't close the bubble
4.navigate to some different sites
5.Enter any credentials on the second site , But do not click on login.
6.Before clicking on login , click save button on the bubble.

It will save the password of first site to second site(wrong site)

Please let me know if you not able to re create it.

Comment 21 by vasi...@chromium.org on Tue, Nov 2, 2021, 12:47 PM EDT

But that's expected. You didn't login on the second site yet. What else could see in the open bubble?

Comment 22 by chakr...@gmail.com on Tue, Nov 2, 2021, 12:52 PM EDT

The problem is, it is saving the password of first site to second site.

So when the user tries to login to second site on some other day.(With wrongly saved password)

He will be exposing the credentials to wrong site.(Without his knowledge)

Comment 23 by chakr...@gmail.com on Tue, Nov 2, 2021, 1:02 PM EDT

If user clicked on save button before clicking on login button in the second site.(After entering the credentials)

The bubble saves the password of first site to second site.

So far the credentials are not exposed to second site.(wrong site)

Now after sometime,

If user visit the second site, the browser automatically brings the wrongly saved password of first site.

If he clicks on login button , he will expose his credentials of first site to second site.

Please let me know if you need additional details.

Comment 24 by chakr...@gmail.com on Tue, Nov 2, 2021, 1:06 PM EDT

Not only password both username and password.(Entire credentials)

Comment 25 by Git Watcher on Thu, Nov 4, 2021, 6:36 AM EDT

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/057e949aee5ce6c8881208e818ec23abb4e126b0

commit 057e949aee5ce6c8881208e818ec23abb4e126b0
Author: Vasilii Sukhanov <vasilii@chromium.org>
Date: Thu Nov 04 10:35:32 2021

Hide the password bubble when the tab controller changes its state.

Currently the bubble stays open until the user explicitly closes it. It
is a problem when an event occurs in the tab that changes the internal
state of ManagePasswordsUIController. Another login will replace the
existing bubble. However, some other cases cause problems:
- User types into a password field. Manual fallback replaces the origin
in the controller.
- User logs in on a "Never save" site.

The password bubble stays currently open. The CL closes the bubble in
those situations.

~~Bug: 1262953~~
Change-Id: I314b248a186b41ab55925d452aed6ec6001740dc
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3259631
Commit-Queue: Vasilii Sukhanov <vasilii@chromium.org>
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Commit-Position: refs/heads/main@{#938210}

[modify]
https://crrev.com/057e949aee5ce6c8881208e818ec23abb4e126b0/chrome/browser/ui/passwords/manage_passwords_ui_controller.h
[modify]
https://crrev.com/057e949aee5ce6c8881208e818ec23abb4e126b0/chrome/browser/ui/passwords/manage_passwords_ui_controller_unittest.cc
[modify]
https://crrev.com/057e949aee5ce6c8881208e818ec23abb4e126b0/chrome/browser/ui/passwords/manage_passwords_ui_controller.cc

Comment 26 by Git Watcher on Tue, Nov 9, 2021, 2:47 PM EST

Status: Fixed (was: Available)

The following revision refers to this bug:
https://chromium.googlesource.com/chromium/src/+/155a965de2b7ebf7ccac9695a66a1b7ddba198c7

commit 155a965de2b7ebf7ccac9695a66a1b7ddba198c7
Author: Vasilii Sukhanov <vasilii@chromium.org>
Date: Tue Nov 09 19:46:06 2021

Hide the save & generate password bubbles more easily.

The password generation bubble will be closed
- if it loses focus (note that it's open without focus) or
- 30 seconds after it was open automatically.
The bubble is a pure confirmation and not very useful for the users.

The save bubble will be closed when it loses focus iff it was open
manually

manually.
Related changes from the past
- https://chromium-review.googlesource.com/c/chromium/src/+/2799692
- https://chromium-review.googlesource.com/c/chromium/src/+/2848390

~~Fixed: 1262953~~
Change-Id: Ib51f76f3630458a678e85a97aa589fa227258292
Reviewed-on: https://chromium-review.googlesource.com/c/chromium/src/+/3270674
Commit-Queue: Vasilii Sukhanov <vasilii@chromium.org>
Reviewed-by: Mohamed Amir Yosef <mamir@chromium.org>
Cr-Commit-Position: refs/heads/main@{#939960}

[modify]
https://crrev.com/155a965de2b7ebf7ccac9695a66a1b7ddba198c7/chrome/browser/ui/views/passwords/password_generation_confirmation_view.cc
[modify]
https://crrev.com/155a965de2b7ebf7ccac9695a66a1b7ddba198c7/chrome/browser/ui/views/passwords/password_save_update_view.cc
[modify]
https://crrev.com/155a965de2b7ebf7ccac9695a66a1b7ddba198c7/chrome/browser/ui/views/passwords/password_generation_confirmation_view.h

Comment 27 Deleted

Comment 28 Deleted

Comment 29 by manapati@google.com on Wed, Nov 10, 2021, 6:15 AM EST

Verified the Fix on Mac(12.0,11.6.1), Win(7,10 & 11) and Linux using latest Canary : 98.0.4697.0

After performing the above steps observed that:
1.When user tries to enter credentials normally in a particular website and hits Key icon and tries to navigate to another site,The "Save Password promo ?" will be automatically closed.
2.When user successfully logins to a particular web site ,The "Save Password promo ?" will appear later if he navigates to another website still promo will be available but in the second web site after trying to give password, The credentials in promo of the first website will be closed.
3.When user successfully logins to a particular web site ,The "Save Password promo ?" will appear, Later if he navigates to any website still promo appears with the credentials of the first web site then if user clicks save button then the credentials will be saved for the first web site.
Hence the fix is working as expected.Adding the verified labels.

Please refer attached screen cast below:
screen cast 1:
https://drive.google.com/file/d/1HFxI66G-0SnfAJcm59Vf0eoLMkm6wD_E/view?usp=sharing

screen cast 2:
https://drive.google.com/file/d/1wbfs7tu8aoIYb9fm2GhKgKynsw9L0ueJ/view?usp=sharing

Thank you..!

Comment 30 by chakr...@gmail.com on Wed, Nov 10, 2021, 11:50 AM EST

Hi team,

I just wonder why there is no reward panel lable is not yet given for this bug

I just wonder why there is no reward panel lable is not yet given for this bug.

Any update regarding reward?

Please share your thoughts.

Thanks,
Chakravarthi

Comment 31 by cthomp@chromium.org on Wed, Nov 10, 2021, 12:14 PM EST

Cc: cthomp@chromium.org

vasilii@ do you have an updated assessment of this bug after fixing it, per the questions raised in Comment #3?

Comment 32 by chakr...@gmail.com on Thu, Nov 11, 2021, 1:01 AM EST

Hi Team,

It should be considered as severe security bug, i have listed few points, Please have a look

There is more chance that users might have already leaked their credentials from one site to other site. (Both via automatically opened bubble flaw and manually opened bubble flaw)

This leakage has happened because of the improper restriction in bubble.

Also, if this is not fixed now, there is huge chance that millions of credentials could have exposed in future.

And if this bug went to public there is huge change that many top organisation might start misuse this as per comment 11.

And more than any of the above points , this bug is potential enough to broke the trust, Which user has on the password manager team over the years.

I am just looking for the answers, whether the work which i have done here is valuable to the team or not.(Answers in the form of reward :P)

Please let me know when you get time.

Have a good day :).

Thanks,
Chakravarthi

Comment 33 by vasi...@chromium.org on Thu, Nov 11, 2021, 4:36 AM EST

The bug could lead to a password being saved for a wrong site. However, the flow is very specific:
- Login on a site A and don't touch the password bubble
- Navigate to site B.
- Type into a password form on the site B.
- Click "Save" in the bubble. The password for site A is saved for the site B.

The bug isn't happening if

- User successfully logins on the site B or
- User types not into the password form on site B.

Comment 34 by chakr...@gmail.com on Thu, Nov 11, 2021, 5:54 AM EST

The google chrome is been used by more than 2.5 billion users.

If we take, just 0.1% users who might have encountered this bug.(There will be more)

And saved the credentials on wrong site.

This exposure will come around 2 million credentials.

And if we have not fixed it now, i am pretty sure that the exposure will we more than 10 million.

So basically we stopped this huge leakage of credentials.

What is stopping you from considering this as a high severity bug?

Share your thoughts.

Thanks,
Chakravarthi.

Comment 35 by chakr...@gmail.com on Thu, Nov 11, 2021, 11:01 PM EST

Hi Team,

Any update regarding the reward eligibility?

If this kind of issues qualifies for reward, it will be worth my time to test other functionalities.

Otherwise i will try something else.Instead of spending time on this.

Please let me know.

Thanks,
Chakravarthi.

Comment 36 by sheriffbot on Fri, Nov 12, 2021, 12:42 PM EST

Labels: reward-topanel

Comment 37 by cthomp@chromium.org on Fri, Nov 12, 2021, 7:09 PM EST

Labels: Security_Severity-Low Security_Impact-Stable Type-Bug-Security

Thanks vasilii@ for fixing this bug and for helping assess the impact.

This doesn't neatly fit into our severity levels for security bugs, but it does feel like there is a risk of this bug causing cross-origin credential leakage. "Medium severity" states "This includes [...] exposure of sensitive user information that an attacker can exfiltrate." However, this is mitigated by requiring a fairly specific invocation sequence with explicit user actions that I think reduce this to at most low severity. In practice, I'd expect this to result in a mostly-benign cross-origin leak, as it seems difficult for a malicious site to cause a user to trigger this flow and ensure they are on the receiving end of the mis-attributed credentials, and to know which site they were intended for (they'd perhaps need to combine this with some sort of history leak bug). I do think it is worth marking this as a security bug and sending it to the panel for evaluation though.

Chakravarthi: Your attention to bugs and sending reports to Chrome is very appreciated! One note is that we have limited bandwidth for looking into bugs, so brief silence on a bug is not us ignoring you, just us being busy. I'd say that even if the

bandwidth for looking into bugs, so brief silence on a bug is not us ignoring you, just us being busy. I'd say that even if the panel decides to not reward for this bug, it is still worth poking around at these kinds of origin-state mixups in feature logic, for the password manager and for other areas in Chrome, as these can very often be security bugs. If you want to learn more about how we think about what is or isn't a security bug, or how we think about the severity of security bugs, I'd recommend reading through our security FAQ [1] and severity guidelines [2]. Thanks again, and happy bug hunting!

[1] https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/faq.md
[2] https://chromium.googlesource.com/chromium/src/+/refs/heads/main/docs/security/severity-guidelines.md

Comment 38 by chakr...@gmail.com on Fri, Nov 12, 2021, 8:54 PM EST

cthomp@ Thank you soo much for the brief explanation..Very much appreciated :)

Comment 39 by sheriffbot on Mon, Nov 15, 2021, 1:46 PM EST

Labels: Restrict-View-SecurityNotify

Comment 40 by chakr...@gmail.com on Sat, Nov 27, 2021, 11:54 AM EST

Hi team any update?

Comment 41 by chakr...@gmail.com on Sat, Nov 27, 2021, 12:03 PM EST

I have noticed that the bubble stays open while doing the sign up on any website.

So if user signed up on any webiste and on the same tab if he navigate to other website and fill login form . And clicks the save button ..The password is getting saved to other website..

I am not sure whehter the given fix will work for this scenario also.. So for a safer side it would be better to test the same on the fixed version of chrome...

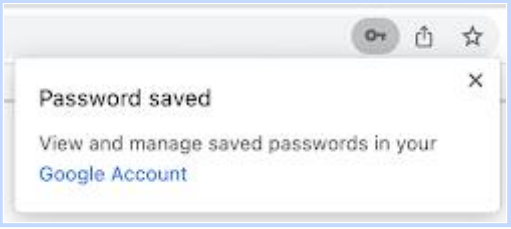
Please let me know if you need any additional details..

Thanks,
Chakravarthi.

Comment 42 by vasi...@chromium.org on Tue, Dec 7, 2021, 5:56 AM EST

What bubble do you see on sign up? If you are talking about password generation then there is no "Save"button.
This bug is fully fixed.

Screen Shot 2021-12-07 at 11.55.54.png
43.8 KB View Download



Comment 43 by chakr...@gmail.com on Tue, Dec 7, 2021, 7:46 AM EST

Hi Vasilii,

Thanks for the reply.

Yes i was referring the password generation bubble while doing the signup

Yes I was referring the password generation bubble while doing the signup.

However, i got one doubt after seeing your comment 42.

If there is no save button, how can they confirm whether they want to save a password or not.

Is it like we are going to save all the passwords or we implemented any new method to get confirmation from user.

Also i wanted to let you know about one more scenario ,

Where that the password bubble will get automatically opened,

I have noticed that the password bubble automatically pops up, while resetting the password also.

So after resetting the password and on the same tab if the user navigate to other website and fill login form . And clicks the save button .The password is getting saved to other website..

So it would be better to test that scenario also.

I just wanted to let you know about, Some of the other scenarios where the password bubble automatically gets opened.

Scenarios when the password bubble automatically open up,

1.When login to new website with valid credentials.
2.While doing the signup on new website.
3.While updating the password of any website using password reset functionality of the website.

If the the given fix works for all the above scenarios, I am good with it.

Please have a look when you get time.

Have a good day.

Thanks,
Chakravarthi.

Comment 44 by vasi...@chromium.org on Fri, Dec 10, 2021, 5:36 AM EST

As I said above the bug is fully fixed. Do you have a concrete flow in M97 that exposes the problem?

Comment 45 by chakr...@gmail.com on Fri, Dec 10, 2021, 6:07 AM EST

@vasiili,

Are you asking for detailed steps?

I tested them in Version 96.0.4664.93.

I can't test them in updated version.(Because i don't have access to future builds)

If you need detailed steps for those scenarios, i can provide it.

But, as i said earlier i have tested them only in 96.0.4664.93.

Please let me know if you need detailed steps.

Have a good day.

Thanks,
Chakravarthi

Comment 46 by amyressler@chromium.org on Tue, Jan 4, 2022, 12:07 PM EST

Labels: Release-0-M97

Comment 47 by amyressler@google.com on Tue, Jan 4, 2022, 1:35 PM EST

Labels: CVE-2022-0120 CVE_description-missing

Comment 48 by chakr...@gmail.com on Fri, Jan 7, 2022, 7:50 AM EST

Team any update regarding the reward?

Can i get approx ETA for panel decision?

Comment 49 by chakr...@gmail.com on Wed, Feb 2, 2022, 7:42 PM EST

Can i do some small writeup regarding the bug?

Can someone tell me long long will take for VRP DECISION?

Comment 50 by sheriffbot on Wed, Feb 16, 2022, 1:30 PM EST

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 51 by chakr...@gmail.com on Sat, Mar 19, 2022, 1:19 AM EDT

Can i do some small writeup regarding the bug?

Can someone tell me how long will it take for VRP DECISION?

Comment 52 by amyressler@chromium.org on Mon, Mar 21, 2022, 3:53 PM EDT

Please accept our sincere apologies for the delay in getting you a reward decision. We have been working through that backlog and have been trying to balance new, high severity decisions with older, lower severity ones and we just hadn't gotten to yours yet.
We will hopefully be this issue through the VRP Panel and making a reward decision soon.

In the meantime, the bug was publicly disclosed (made 'allpublic') on 16 February, so you are free to do a write up at this time without impact to your VRP reward.

We sincerely appreciate your patience while we work through our backlog.

Comment 53 by amyressler@chromium.org on Mon, Mar 21, 2022, 3:54 PM EDT

Labels: -Restrict-View-Google

Comment 54 by amyressler@google.com on Wed, Mar 23, 2022, 3:46 PM EDT

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 with any questions.
****

Comment 55 by amyressler@chromium.org on Wed, Mar 23, 2022, 4:19 PM EDT

Hello! The VRP Panel has decided to award you $500 for this report as a thank you for reporting this issue and allowing us to fix this in away that improves the user experience of password usage in Chrome. The reward amount was decided based on the very unlikely and non-standard workflow to leverage this issue. Thank you for your efforts and, again for reporting this issue to us.

Comment 56 by chakr...@gmail.com on Wed, Mar 23, 2022, 9:05 PM EDT

Wow thank you ..:)

Comment 57 by amyressler@google.com on Fri, Mar 25, 2022, 5:27 PM EDT

Labels: -reward-unpaid reward-inprocess

Comment 58 by amyressler@chromium.org on Fri, Jul 29, 2022, 5:36 PM EDT

Labels: -CVE_description-missing CVE_description-submitted