To CEO

Security Operation Center

Global Comm

Password Manager – Vulnerability Advisory

Summary of the Vulnerabilities poses by Password Managers

Password managers contains the ability to autofill the login page and submit the passwords and other credentials. Sometime it requires manual interaction of the user and sometimes it just fills the space without any manual interaction. There are various policies followed by the password managers regarding the protection of the user credentials.

But the attacker can leverage the weaknesses in the password managers and can be successful to exfilterate the user creds and other data. There are various use cases where the attacker and the victim are both connected to the same rouge Wi-Fi router and the attacker is controlling the Wi-Fi. In many cases the user doesn't even need to login into target websites.

The another scenario where the user can be vulnerable to the password manager attack is when the user has its all password sync to all of its personal devices. In that case even if the user has hardened the security on the personal laptop and device and he is using some different device like its tab or mobile, the same password manager attack is applicable.

Execution of the JavaScript is the most common scenario the attacker will use to exfilterate the user creds. Somehow the attacker will trick the user to access the vulnerable website and there will be some iframe which will require user login and password manager's autofill just fills spaces in the iframe and JS script will be able to fetch the creds.

The other Weaknesses or attack surfaces which some of the password managers have or some of them does not can be as following:

1. Trusting the webpages or links sourcing same domain
2. When webpage is http but the login page is https or any other https component on the http page
3. When form action attribute is not same and password managers still allows to autofill and submit.
4. Autocomplete attribute: this was meant to defend the autofill feature but some password manager is vulnerable to this policy.
5. When certificate is expired or there is some issue with https some password managers would still be able to autofill the creds.
6. When password field name is different, some password managers don't able to detect that or recognize that and just fill the creds with autofill.
7. Iframe injection can be done as described above.

So these are the vulnerabilities that the password managers could have on your system. Hardening the websites with WAF or carefully selecting the password manager is really important. These third party tools can expose the user data and other creds to an attacker even after you invest everything for your security on your personal devices with antiviruses and firewalls.

Impact on privacy

The vulnerability in password managers if exploited could have major impact on the enterprises and the privacy of the user. The kind of the data and content that password managers store is very sensitive and in some cases could be a major attack vector in achieving bigger targets. Further it depends on the type of industry and the app that uses the password manager and for which user the password managers are storing the creds.

- Let’s say some admin level of user is sipping the coffee in the Starbucks and prefers to work along with sipping coffee. The manager tries to connect to the WiFi router and by some that router is affected and controlled by an attacker. The attacker will be able to exfiltrate the **admin level privileges** and could further use it to make a bigger impact.
- In the case of the home usage of the devices, many users prefer to use password managers and store their passwords of social websites they visit with the password manager. Let’s say the same user visits some vulnerable website or torrent website in parallel. The attacker can use JavaScript and exfilterate the data from the password manager which helps the victim to login **into social sites**. Once the attacker has all these creds, he can access all these websites and can access everything which should be personal to the user.
- The another use case which is pretty common and can be found with every other user is **banking services**. Many home users are not aware of the security implications of these type of vulnerabilities and prefer convenience over security. When they try to login in the bank website and the banking website let’s say, using the https component over http or was previously using different protocol when the password manager saved the creds, the user exposing himself to the vulnerability in password manager and the

attacker can easily gain the access to the user bank account and can further process the fund transfer.

A strategy to weaponize this threat and use it during a Penetration Testing engagement

So there are many ways a pentester can implement to exploit one of the vulnerabilities that exists in the password manager. One of the ways that was described in the paper would be as following:

(Considering the case when the attacker is already sitting in the network and sniffing on the network traffic that normal user is going through. This can be done in many ways such as SSLStrip or control over rogue router or Wifi hotspot with same SSID)

Assuming the above condition true, we will then need something to weaponized to pull off this kind of attack.

- Let's say the victim connects to the network which is being control of the attacker. The attacker a further sniff on the network traffic and manipulate the packets being sent from victim machine.
- Victim tries to connect to the legit website, let's say, xyz.com. the attacker then able to sniffs on the traffic and manipulate the response to victim machine.
- The attacker responds with the redirect request to the pqr.com which is vulnerable website. The vulnerable website might contain JavaScript which will have a login form.
- Password manager having the weaknesses for auto filling will not validate the page and check for the policies. The JavaScript running on the page will exfilterate the data to the attacker's server.
- To further exfilterate other user creds, the attacker can keep on sending the redirect requests to the victim and password manager will keep auto filling the vulnerable login pages.

- At the end, the attacker will return the actual genuine page to the victim. If the password manager doesn’t have any policy enabled which requires the manual human interaction with user cred submission, the process will be so fast that there will less indication of the attack.