[Critical bug]Fuelet Wallet password replacement attack

Author: nolan@exvul.vom

X:@ma1fan

Description

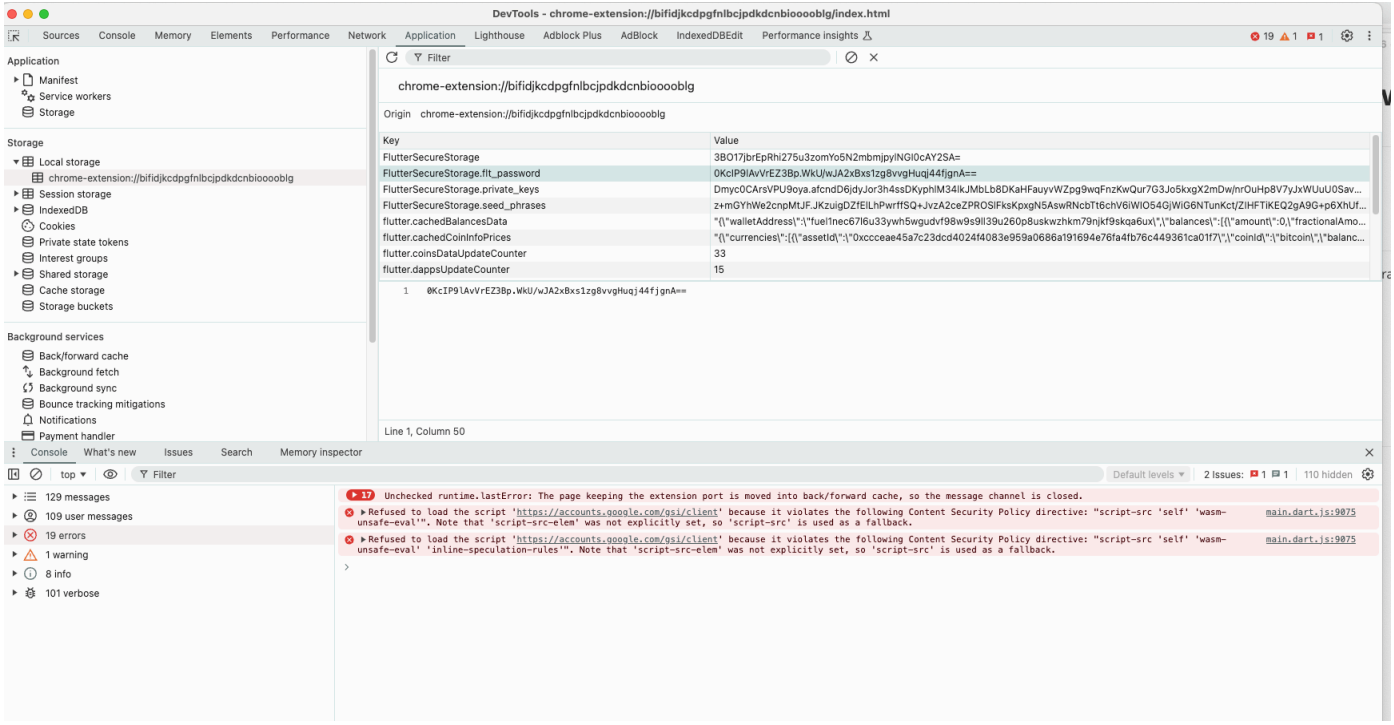
attacker can unlock user's wallet and stolen users private key or phrase words by replacement the ciphertext .even the wallet is locked, still can decrypt the viticm's private key and phrase words!!!

so this is a Critical bug.

Detail

the wallet store the password ciphertext in localstorage,also the private keys phrase words.

the wallet only verify the password is vaild or not, and if the password is right will decrypt the private key or phrase words, the bad thing is when decrypt the private key or phrase words the wallet not verify the password can be decrypt success or not. if attacker can use a vaild ciphertext and replacement the viticim's ciphertext will bypass the password verify and attacker can decrypt the viticim's private key and phrase words ,



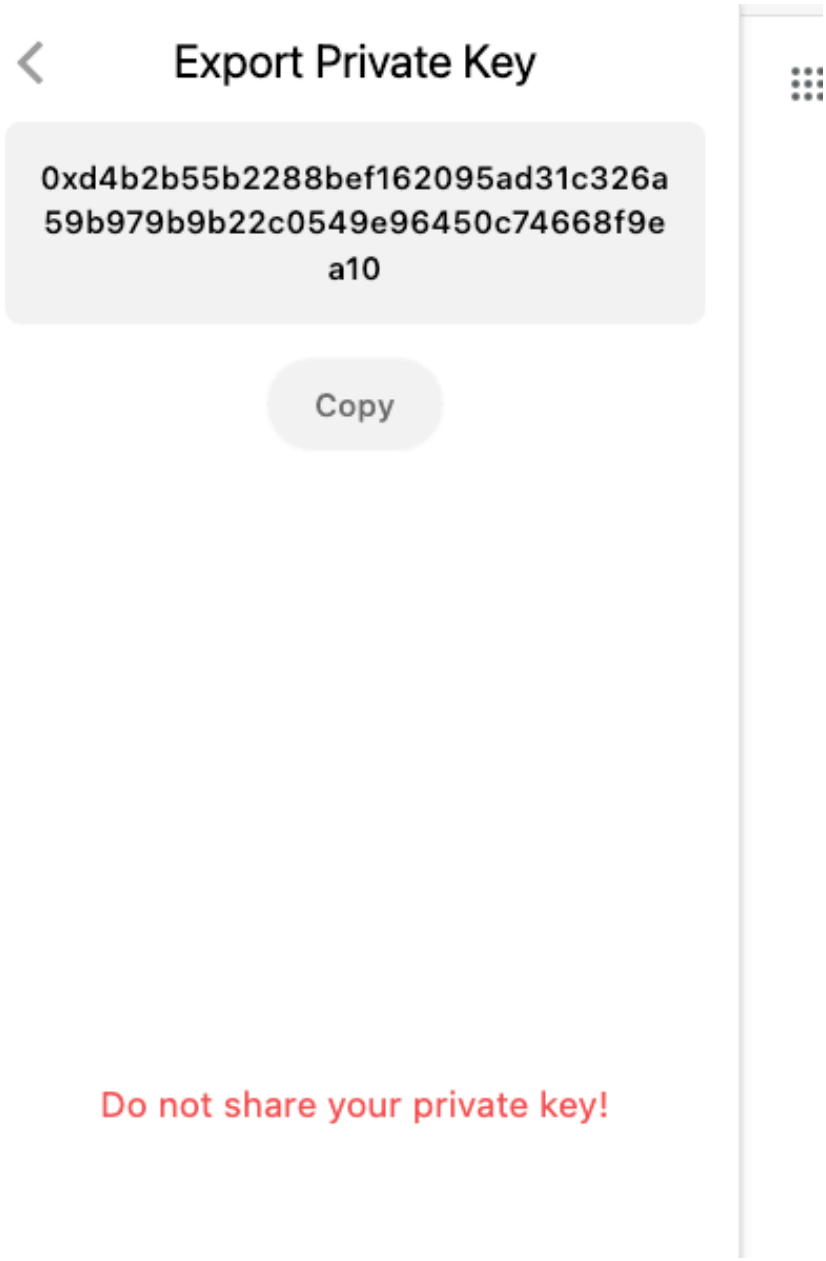
Exploit steps:

1.**Attacker** create a wallet with password `123456`

Ciphertext:

`dH6MZkI7ysR3dEd1.JDjijPD46loY5WKvki7bEV/B48d2hA==`

`0xd4b2b55b2288bef162095ad31c326a59b979b9b22c0549e96450c74668f9ea10`



2.vicitm create a wallet with password `00000000`

3.Now you can replacment the victim's password Ciphertext with Attacker's password Ciphertext.

4. and then you can unlock the victim's wallet with attacker's password `123456` .

   and export the vicicim's privatekey, for now you can see the privatekey is victim's private key.

   So this means you can stolen user's privatekey and phrase word!!!

   also means attacker can stolen all the users funds**

Impact:

1. unlock the arbity wallet
2. Stolen user's privatekey
3. Stolen user's phrase words