

[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 victim'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 ,

The screenshot displays the Chrome DevTools interface for a Chrome extension. The top panel shows the 'Application' tab, specifically the 'Storage' section. Under 'Local storage', the extension's storage area is expanded, revealing a table of keys and values. The keys include 'FlutterSecureStorage', 'FlutterSecureStorage.ffi_password', 'FlutterSecureStorage.private_keys', 'FlutterSecureStorage.seed_phrases', 'flutter.cachedBalancesData', 'flutter.cachedCoinInfoPrices', 'flutter.coinDataUpdateCounter', and 'flutter.dappsUpdateCounter'. The values are mostly long alphanumeric strings, with some containing JSON-like structures for balances and coin data.

The bottom panel shows the 'Console' tab with several error messages. The first error is a warning about an unchecked runtime.lastError. The subsequent two errors are red, indicating Content Security Policy (CSP) violations. Both errors state: 'Refused to load the script 'https://accounts.google.com/gsi/client' because it violates the following Content Security Policy directive: "script-src 'self' 'wasm-unsafe-eval'". Note that 'script-src-elem' was not explicitly set, so 'script-src' is used as a fallback.' The source file for these errors is 'main.dart.js:9075'.

Key	Value
FlutterSecureStorage	3B017JbrEpRH275u3zomYo5N2mbmjpyNGl0cAY2SA=
FlutterSecureStorage.ffi_password	0KciP9IAwVrEZ38p.WkUJwJA2x8xs1zg8vvgHuqj44fjgnA==
FlutterSecureStorage.private_keys	DmycOCarsVPUB9oya.afendD6jdyJor3h4ssDKyphIM34lkJMbLb8DKaHFauyrvWZpg9wqFnzKwQu7G3Jo5kxgX2mDwJhrOulH8V7yJxWUuU0Sav...
FlutterSecureStorage.seed_phrases	z+mGYhWe2cnpMtJfJKzuigDZIElJhPwrtfSQ+JvzA2ceZPROSIFksKpgN5ASwRncbT6chV6WIO54QlWiG6NTunKct/ZHfTIKEQ2gA9G+p6XhUf...
flutter.cachedBalancesData	{\"walletAddress\":\"fueltec67b6u33ywh5wgudvf98w9e9l39u260p8uskwzhkm79njkt9skq6ux\", \"balances\": [{\"amount\": 0, \"fractionalAmo...
flutter.cachedCoinInfoPrices	{\"currencies\": {\"assetid\": \"0xcceae45a7c23dc04024f4083e959a0686a191694e76fa4b76c449361ca01f7\", \"coinid\": \"bitcoin\", \"balanc...
flutter.coinDataUpdateCounter	33
flutter.dappsUpdateCounter	15

Exploit steps:

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

Ciphertext:

`dH6MZkI7ysR3dEd1.JDji jPD46loY5WKvki7bEV/B48d2hA==`

`0xd4b2b55b2288bef162095ad31c326a59b979b9b22c0549e9
6450c74668f9ea10`



Export Private Key



```
0xd4b2b55b2288bef162095ad31c326a  
59b979b9b22c0549e96450c74668f9e  
a10
```

Copy

Do not share your private key!

2.victim 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 victim'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

