TBB

Security Code Validation

https://twitter.com/VidarTheAuditor - 23 February 2021

Overview

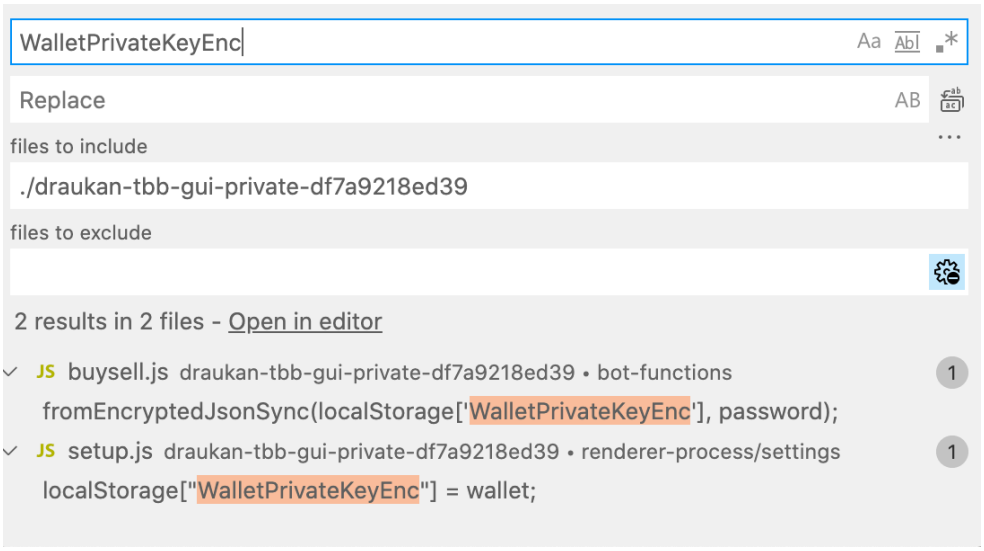
Project Summary

Project Name	TBB
Description	Bot software
Platform	**Electron, node.js**
Source	Provided as private repo

Summary

We have been given the source code of the bot software to validate the usage of private key information.

Private key is used in two places in the codebase: buy sell.js (which is encrypted) and setup.js



The logic concerning private key usage is as follows:

- Software validates entered private key and encrypts it using the provided password utilising Ether.js functionality to store wallet information. (setup.js)
- The private key is kept as Ether JSON wallet in an encrypted form in a local storage (Chrome).
- In order to sign transactions wallet is read from local storage and decrypted using the password provided by the user. (buysell.js)

The private key is not used outside of that flow and it is stored in Chrome local storage in an encrypted form.

We have verified the source code of the encrypted (JSC) files and generated MD5 for them.

MD5 (buysell.jsc) = 4d30cb1ae7f9e34a121f2c5332d5f05a

MD5 (processor.jsc) = 7a38e50dc8ccfcabd91a1d3fb6eca771

We strongly advice to verify the integrity of those files before providing private key information to the installed software.

Disclaimer

The information appearing in this report is for general purposes only and is not intended to provide any legal security guarantees to any individual or entity. As one review is not enough to provide 100% security against any attacks or bugs, it is **strongly advisable** to conduct **more reviews or/and audits**.

The report does not provide personalised investment advice or recommendations, especially does not provide advice to conclude any transactions and it does not provide investment, financial, legal or tax advice.

We are not responsible or liable for any loss which results from the report.

The report should not be considered as an investment advice.