a&r infotech inc.
www.arinfotech.com

KWHCoin Token Sale Audit

The KWHCoin team asked us to review and audit their KWHCoin Token Sale contracts. We looked at the code and now publish our results. Here's our assessment and recommendations, in order of importance.

Scope of the Audit

The audit was based on the Ethereum Virtual Machine (EVM) after EIP-150 and solidity compiler 0.4.17.
The scope of the audit is limited to the following source code files:
• KWHCoin.sol

Critical Severity

No issues of critical severity.

High Severity

No issues of high severity.

Medium Severity

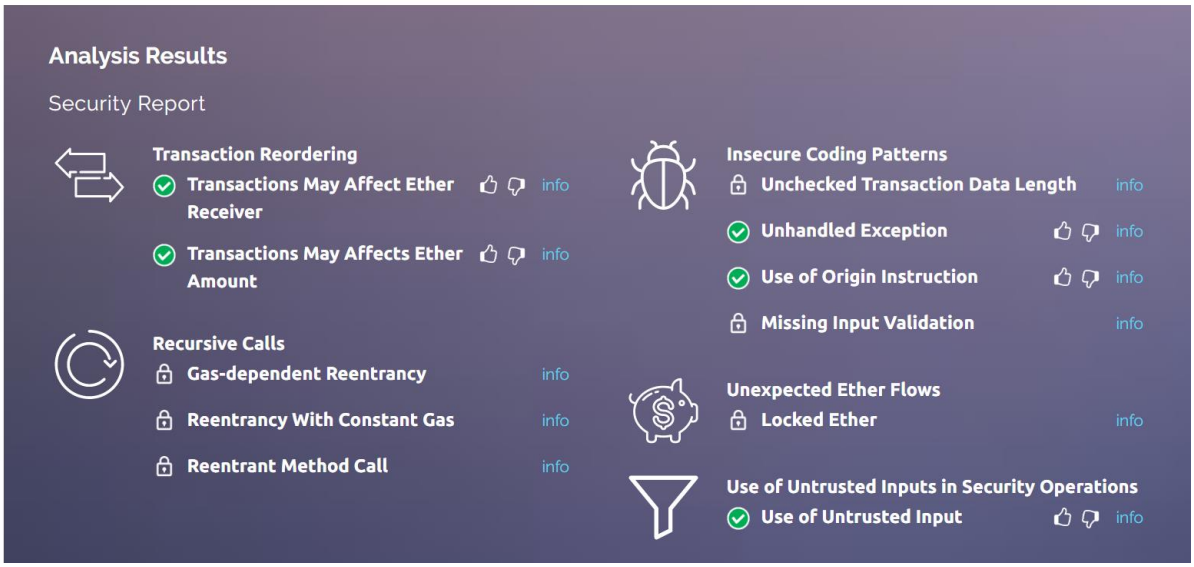
No issues of Medium severity.

Low Severity

No issues of low severity.

List of potential attacks tested

1. Audit was performed using 5 accounts with 100 ETH each.
2. Correct use of function visibility modifiers
3. Call stack attack
4. DoS with unexpected throw
5. Is there re-entry possibility and how it behaves on re-entry
6. How it behaves if loops run out of gas
7. How it behaves if stack limit is reaches
8. Transaction-Ordering Dependence
9. Forced balance update
10. Loop length and gas manipulation
11. Integer division round down
12. Malicious libraries



Notes & Additional Information

13. Consider using require instead of if (...) throw. throw has been deprecated in latest Solidity.
14. During compilation there is a warning
15. We would recommend including the extra contract, and replacing the usage of call for a Solidity function call.

Conclusion

The smart contract has been analyzed under different aspects, with different open-source tools as well as our fully fledge proprietary in house tool. Overall, we found that KWHCoin employ very good coding practices and has clean, documented

code. We have no remaining security concerns about the KWHCoin smart contracts, as all detected issues were either fixed or addressed.