SMART CONTRACT AUDIT REPORT

For

Cryptoxygen Token (Order # 26DEC2018A)

Prepared By: Yogesh Padsala

Prepared on: 26/12/2018

Revised on: 03/01/2019

audit@etherauthority.io

Prepared For: Cryptoxygen OU

https://www.cryptoxygen-stage.com

Table of Content

1. Disclaimer

The audit makes no statements or warranties about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only.

2. Overview of the audit

The project has following file:

- CryptoxygenToken.sol

The source code present at:

https://kovan.etherscan.io/address/0x45d75933d0345d65c1506153b59c0b08b5b4d817#code

It contains approx **378** lines of Solidity code. All the functions and state variables are **not** well commented using the natspec documentation, but that does not raise any vulnerabilities. But It would have increased the readability. https://github.com/ethereum/wiki/wiki/Ethereum-Natural-Specification-Format

The audit was performed by Yogesh Padsala, from EtherAuthority Limited. Yogesh has extensive work experience of developing and auditing the smart contracts.

The audit was based on the solidity compiler 0.5.2+commit.1df8f40c with optimization enabled compiler in remix.ethereum.org.

This audit was also performed verification of the details exist in whitepaper: https://www.cryptoxygen-stage.com/assets/whitepaper/cryptoxygen.pdf

Quick Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	Passed
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert() misuse	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	“Out of Gas” Attack	Passed
Business Risk	Evil mint/burn	Passed
	The maximum limit for mintage not set	Passed
	“Fake Charge” Attack	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed
Auto Fuzzing		Passed

Overall Audit Result: PASSED

3. Attacks tested on the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

3.1: Over and under flows

This contract **does** check for overflows and underflows by using OpenZeppelin's SafeMath to mitigate this attack, and all the functions have strong validations, which prevented this attack.

3.2: Short address attack

Although this contract **is not vulnerable** to this attack, it is highly recommended to call functions after checking validity of the address from the outside client.

3.3: Visibility & Delegatecall

Delegatecall is not used in the contract thus it does not have this vulnerability. And visibility is also used properly at most places. Although visibility is not specified at some places , which are discussed below.

3.4: Reentrancy / TheDAO hack

Use of “require” function and Checks-Effects-Interactions pattern in this smart contract mitigated this vulnerability.

3.5: Forcing ether to a contract

Here, the Smart Contract’s balance has never been used as guard, which mitigated this vulnerability

3.6: Denial Of Service (DOS)

There is no process consuming loops in the contracts which can be used for DoS attacks. Also, there is no progressing state based on external calls, and thus this contract is not prone to DoS.

4. Good things in the smart contract

4.1 Declaring variables as constant

The value of variables at line number #309, #310, #312, #313, #314, etc., is not expected to change. Thus it is good thing to declare them as constant, which helps reduce the gas cost.

4.2 Admin control over token transfer

```
modifier isRunning {
    assert (!stopped);
    _;
}
```

This is always considered a great practice for the owner to halt or resume the token transfer and other process. This is really useful in any unexpected event or any controlled token transfer logic.
Here, owner can stop token transfer by calling stop() function, and resume it back again by calling start() function.

4.3 Checks-Effects-Interactions pattern

While transferring tokens, this contract does all the process first and then transfers them. The same while doing other process too. This is very good practice which prevents malicious possibility. For example: transferFrom() function.

4.4 Functions input parameters passed

The functions in this contract verifies the validity of the input parameters, and this validations cannot be by-passed in anyway.

5. Critical vulnerabilities found in the contract

Critical issues that could damage heavily the integrity of the contract. Some bug that would allow attackers to steal ether is a critical issue.

=> No Critical Vulnerabilities found

6. Medium vulnerabilities found in the contract

Those vulnerabilities that could damage the contract but with some kind of limitations. Like a bug allowing people to modify a random variable.

=> No Medium Vulnerabilities found

7. Low severity vulnerabilities found

Those do not damage the contract, but better to resolve and make code clean.

7.1: Non-initialized return value

The preSale() function at line number #346 doesn't initialize return value. This is not a big issue as default value will be returned. But it is good practice not to specify returns in function signature, if return value is not required.

7.2: Implicit visibility level

At line number #111, #112, #316, #317, #318, #319, #321, #322, #323, #324, #325, #326, #328, #329, #330, #331, #332, the visibility was not specified explicitly.

Now, this is not a big issue, as it takes default to “internal” for state variables. But it is good practice to explicitly declare the visibility of the state variables.

https://solidity.readthedocs.io/en/develop/contracts.html#visibility-and-getters

8. Gas Optimization Discussion

=> Contract is most optimum for the gas cost

9. Discussions and improvements

9.1 The SafeERC20 Library

This library is not used anywhere in the code. So better to remove it to make code clean, unless there is any intentional use of it.

9.2 Update hard-coded addresses

It is good idea to add a functions which enables owner to update/change founders and developer address. This is useful in case of compromisation of any of those accounts.

9.3 approve() of ERC20 Standard

To prevent attack vectors regarding approve() like the one described here: https://docs.google.com/document/d/1YLPtQxZu1UAvO9cZ1O2RPXBbT0mooh4DYKjA_jp-RLM/edit , clients SHOULD make sure to create user interfaces in such a way that they set the allowance first to 0 before setting it to another value for the same spender. THOUGH the contract itself shouldn't enforce it, to allow backwards compatibility with contracts deployed before

9.4 Custom error message in require() function

It is good idea to specify a custom error message in require function, which can be useful in GUI and error debugging down the road.

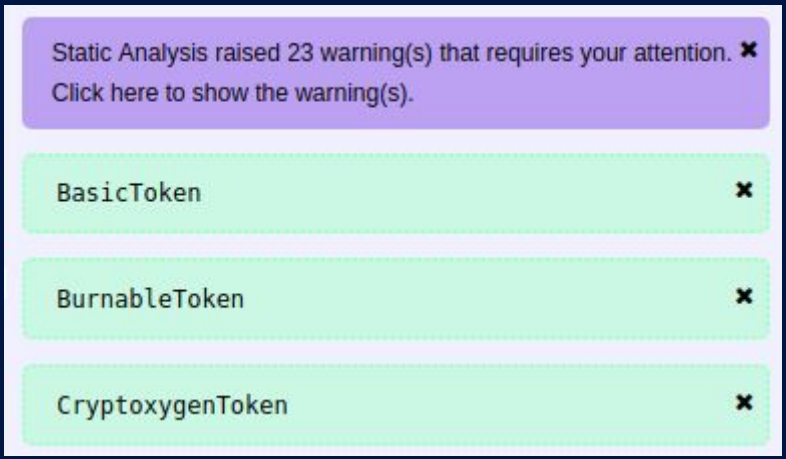
9.5 While using SafeMath library

The SafeMath library is doing the great job to prevent overflow and underflow. However, it is recommended **NOT** to use it when overflow/underflow is impossible. Because please keep in mind that every unnecessary checks contribute to increased gas cost!

10. Summary of the Audit

Overall the code performs good data validations as well as meets the correctness of data according to the information presented in the whitepaper: https://www.cryptoxygen-stage.com/assets/whitepaper/cryptoxygen.pdf

The compiler also displayed 23 warnings:



Now, we checked that the warnings in purple division, are due to their static analysis, which includes like gas estimations and all. So, it is important to supply correct gas values while calling various functions.

Those warnings can be **safely ignored** as should be taken care while calling the smart contract functions.

Please try to check the address and value of token externally before sending to the solidity code.

It is also encouraged to run bug bounty program and let community help to further polish the code to the perfection.