Soteria Smart Contracts

Shiba Classic ERC20 Smart Contract Security Review

August 22nd 2022

[Source Code]

Abstract

In this report, the Soteria Smart Contracts team will determine the security level, the conformity to the ERC20 token standard and the vulnerabilities (if any) of the Shiba Classic (ShibC) ERC20 token.

The final statement on the Security level is only an opinion by the team conducting this review, and is in no way a legal confirmation of the security of the Smart Contract in question.

Any solutions that may be put forward by the Shiba Classic team to fix or prevent issues with the Smart Contract (if any) will be outlined directly below the classing of the severity of the vulnerability.

For those looking to follow along with the Smart Contract, a link to the source code can be found above, and you may find the Smart Contract on the Ethereum Classic Blockchain under this public address:

0x1FDc495289B590e78d455cf7faa6cd804de5Cbc1

Project Details

Blockchain: Ethereum Classic (ID: 61)

Project Name: ShibaClassic

Creator: Unknown (0x8cE6FA726Ba047B7422c67441481c0F92e24C5bD)

Token Standard: ERC20

Token Name: ShibaClassic

Token Symbol: SHIBC

Token Decimal Precision: 18

Token Maximum Supply: 100,000,000,000,000 SHIBC

Vulnerability severity classing

In order to determine the severity of individual vulnerabilities, a classing system must be in place, which is as follows:

Low

Small vulnerabilities which typically have no impact over the course of the lifetime of the Smart Contract, and do not have any impact on the movement of any assets/tokens.

Medium

Unlikely to be dangerous to the Smart Contract, but in the wrong circumstances may lead to failure of one or more of the functions within the Smart Contract. Unlikely to affect the movement of assets/tokens.

Severe

May pose a serious risk to the Smart Contract and its underlying functions if a malicious transaction or malicious transactions are sent to the Smart Contract. May or may not affect the movement of assets/tokens.

Critical

A serious threat to the integrity of the smart contract, which would require an immediate re-deployment with repairs to the protocol as soon as possible. Likely affects the movement of assets/tokens.

ERC-20 Standard Conformity

The ERC-20 standard is a standard that was originally proposed in the Ethereum Improvement Proposal number 20, in which Smart Contracts may want to conform to in order to make the implementation of their fungible token easier for external parties in other applications.

The ShibaClassic token conforms to all items, functions and events included, listed at the EIP-20 standard detail.

Vulnerabilities Found:

Low

Solidity version and Compiler Version

This smart contract uses the Solidity version 0.5.0, which is an older solidity version. This does not affect the Smart Contracts utility or protocol, but may affect gas efficiency and overflow protection typically found in the newer versions of solidity. Thankfully, this smart contract implements OpenZepplin's Safemath protocol which essentially eliminates the possibility for over/underflows in integers or unsigned integers.

Full supply token minting to contract deployer on contract creation

As outlined in the constructor within this contract, all ERC20 tokens belonging to the ShibaClassic contract are minted on the deployment of the contract to the deployer. This means that all tokens in existence were at some point all in one wallet. Since the deployment, these funds have been put into liquidity at the Hebeswap protocol, a clone of the Uniswap V2 protocol, and the liquidity tokens have been burnt to the dead address.

Medium

No vulnerabilities found

Severe

No vulnerabilities found

Critical

No vulnerabilities found

Conclusion and Final Statement

From the information and vulnerabilities found during this review, we believe the creator of the ShibaClassic project has successfully created a safe Smart Contract, along with burning the liquidity which derived from the original minting of all SHIBC in existence. The two vulnerabilities found can be ignored due to their low severity and the solutions that have already been put in place. Additionally, we have found no ownership statements within the contract which would allow for changing of things such as transaction taxes, or other malicious code.

We would like to thank you for reading this document, any feedback may be sent to Soteria Smart Contracts on twitter.

Disclaimer

This report is subject to the terms and conditions (including without limitation, description of services, confidentiality, disclaimer and limitation of liability) set forth in the Services Agreement, or the scope of services, and terms and conditions provided to the Company in connection with the Agreement. This report provided in connection with the Services set forth in the Agreement shall be used by the Company only to the extent permitted under the terms and conditions set forth in the Agreement. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes without Soteria Smart Contracts's prior written consent. This report is not, nor should be considered, an "endorsement" or "disapproval" of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Soteria Smart Contracts to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology. Blockchain technology and cryptographic assets present a high level of ongoing risk. Soteria Smart Contracts's position is that each company and individual are responsible for their own due diligence and continuous security. Soteria Smart Contracts's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

Soteria Smart Contracts