



Smart contracts security assessment

Final report

[Tariff: Standard](#)

TooToken

October 2021



0xguard.com



hello@0xguard.com

Contents

1. Introduction	3
2. Contracts checked	3
3. Procedure	3
4. Known vulnerabilities checked	4
5. Classification of issue severity	5
6. Issues	5
7. Disclaimer	7

Introduction

TooCoin is a burnable BEP20 contract. It is highly dependent on the owner account. If the owner account is compromised, the attacker can mint and sell unlimited amount of token, dropping token price to zero. We recommend securing the owner account using a multisig.

Name	TooToken
Audit date	2021-10-21 - 2021-10-21
Language	Solidity
Platform	Binance Smart Chain

Contracts checked

Name	Address
CoinToken	0x33Fea48c8e842a14c62dF14C83c79E43Dd6386fF

Procedure

We perform our audit according to the following procedure:

Automated analysis

- Scanning the project's smart contracts with several publicly available automated Solidity analysis tools
- Manual verification (reject or confirm) all the issues found by the tools

Manual audit

- Manually analyse smart contracts for security vulnerabilities
- Smart contracts' logic check

Known vulnerabilities checked

Title	Check result
Unencrypted Private Data On-Chain	passed
Code With No Effects	passed
Message call with hardcoded gas amount	passed
Typographical Error	passed
DoS With Block Gas Limit	passed
Presence of unused variables	passed
Incorrect Inheritance Order	passed
Requirement Violation	passed
Weak Sources of Randomness from Chain Attributes	passed
Shadowing State Variables	passed
Incorrect Constructor Name	passed
Block values as a proxy for time	passed
Authorization through tx.origin	passed
DoS with Failed Call	passed
Delegatecall to Untrusted Callee	passed
Use of Deprecated Solidity Functions	passed
Assert Violation	passed
State Variable Default Visibility	passed
Reentrancy	passed
Unprotected SELFDESTRUCT Instruction	passed
Unprotected Ether Withdrawal	passed
Unchecked Call Return Value	passed

Floating Pragma	passed
Outdated Compiler Version	passed
Integer Overflow and Underflow	passed
Function Default Visibility	passed

Classification of issue severity

High severity	High severity issues can cause a significant or full loss of funds, change of contract ownership, major interference with contract logic. Such issues require immediate attention.
Medium severity	Medium severity issues do not pose an immediate risk, but can be detrimental to the client's reputation if exploited. Medium severity issues may lead to a contract failure and can be fixed by modifying the contract state or redeployment. Such issues require attention.
Low severity	Low severity issues do not cause significant destruction to the contract's functionality. Such issues are recommended to be taken into consideration.

Issues

High severity issues

1. Unlimited minting by Owner (CoinToken)

Function mint is restricted by onlyOwner modifier which makes the owner able to mint any amount of tokens to any address. It's considered as High severity since gives to the owner unlimited powers of minting.

Recommendation: There are several ways to mitigate the issue:

1. Renounce ownership of the token (blacklist functionality in such case won't work also).

2. Create a wrapper contract that will limit maximum amount of tokens to minted and transfer ownership to it.
3. Transfer ownership to a multisig account with several independent parties.

Medium severity issues

1. User's Ability of transfer depends on Owner (CoinToken)

Owner is able to restrict users' ability of transfer by blacklisting them (L134, L151). Including to and excluding from the Black-list depend on Owner's decision only (L195).

Low severity issues

1. Lack of error-messages in require() (CoinToken)

No one `require()` function has an error-message, which would explain the reason of a fail.

Recommendation: Consider adding the error-messages.

2. Lack of getOwner() function (CoinToken)

The token lacks the `getOwner()` function required in the BEP20 token standard. We mark the severity of the issue as low because this function is rarely used in the tokens.

Recommendation: Add the required function.

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 0xGuard 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 0xGuard 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.

