Guard

Smart contracts security assessment

Final report

Tariff: Top

Sonik

August 2023

0xguard.com

hello@0xguard.com

Contents

Introduction

The report has been prepared for **Sonik**.

Audited token is an ERC-20 standard token. The Sonik token doesn't have active mint functionality after contract deployment.

The code in the @SONIKDev/SonikTokenContract Github repo was audited in the fc81239 commit.

Name	Sonik
Audit date	2023-08-15 - 2023-08-16
Language	Solidity
Platform	Ethereum

Contracts checked

Name	Address
SonikCoinToken	

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 analyze 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	not 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Outdated Compiler Version	passed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

No issues were found

Medium severity issues

No issues were found

Low severity issues

1. Unused import (SonikCoinToken)

Status: Open

SonicCoinToken contract is derived from the Ownable contract from OpenZeppelin library, but it's functionality never used.

Sonik team comment: The Ownable contract is used to transfer or renounce ownership of the token, but is never used in the token itself.

2. Standard violation (SonikCoinToken)

Status: Open

The ERC-20 token standard requires transfers with zero amount to be processed. The Sonik token reverts all such transfers explicitly.

```
    function _transfer(
        address sender,
        address recipient,
        uint256 amount
    ) internal virtual {
        require(amount > 0, "ERC20: transfer amount zero");
        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");

        uint256 senderBalance = _balances[sender];
        require(
            senderBalance >= amount,
            "ERC20: transfer amount exceeds balance"
        );
        unchecked {
            _balances[sender] = senderBalance - amount;
        }
```

```
        _balances[recipient] += amount;

        emit Transfer(sender, recipient, amount);
    }
```

Recommendation: Comply to the standard.

Sonik team comment: The Sonik Token reverts all such transfers explicitly, this function has been added to protect token holders from Zero-Value Token Transfer Attacks. See more information here https://info.etherscan.com/zero-value-token-transfer-attack/.

Conclusion

Sonik SonikCoinToken contract was audited. 2 low severity issues were found.

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.

0x Guard