// Smart Contract Security Assessment 08.16.2024 - 09.13.2024

Toshi

Toshi

HALBORN

Toshi

Prepared by: HALBORN

Last Updated 10/17/2024

Date of Engagement by: August 16th, 2024 - September 13th, 2024

Summary

100% OF ALL REPORTED FINDINGS HAVE BEEN ADDRESSED

ALL FINDINGS	CRITICAL	HIGH	MEDIUM	LOW	INFORMATIONAL
55	2	1	6	20	26

1. Introduction

Toshi engaged Halborn to conduct a security assessment on their smart contracts beginning on **08-16-2024** and ending on **09-17-2024**. The security assessment was scoped to the smart contracts provided in the **https://github.com/Toshi-The-Cat/toshi-solidity** GitHub repository. Commit hashes and further details can be found in the Scope section of this report. The Toshi codebase in scope **consists mainly of a Presale contract destined to facilitate the sale of tokens before they are listed on exchanges, as well as different multipurpose tokens.**

TABLE OF CONTENTS

2. Assessment Summary

`Halborn` was provided 4 weeks for the engagement and assigned 1 full-time security engineer to review the security of the smart contracts in scope. The engineer is a blockchain and smart contract security expert with advanced penetration testing and smart contract hacking skills, and deep knowledge of multiple blockchain protocols.

The purpose of the assessment is to:

- Identify potential security issues within the smart contracts.
- Ensure that smart contract functionality operates as intended.

In summary, `Halborn` identified some improvements to reduce the likelihood and impact of risks, which were mostly addressed by the `Toshi team`. The main identified issues were:

- **Impossibility to collect LP fees from Locker contract.**
- **Overridden `_update()` function silently blocks dividend distribution.**
- **Missing quote token address verification denies liquidity withdrawal.**
- **Unsafe casting may lead to underflow.**
- **Precision loss due to division before multiplication.**

3. SCOPE

FILES AND REPOSITORY

(a) Repository: toshi-solidity

(b) Assessed Commit ID: f4b23ad

(c) Items in scope:

- src/utils/SafeERC20NoRevert.sol
- src/utils/IterableMapping.sol
- src/interfaces/INonfungiblePositionManager.sol
- src/interfaces/IAntiBot.sol
- src/interfaces/IDividendDistributor.sol
- src/interfaces/IConfig.sol
- src/interfaces/IDividendPayingToken.sol
- src/tokens/BabyTokenFactory.sol
- src/tokens/StandardToken.sol
- src/tokens/Auth.sol
- src/tokens/LiquidityToken.sol
- src/tokens/LiquidityTokenFactory.sol
- src/tokens/DividendDistributorFactory.sol
- src/tokens/AntiBot.sol
- src/tokens/BabyTokenDividendTracker.sol
- src/tokens/BuyBackToken.sol
- src/tokens/AntiBotFactory.sol
- src/tokens/DividendPayingToken.sol
- src/tokens/BabyToken.sol
- src/tokens/BaseToken.sol
- src/tokens/BuyBackTokenFactory.sol
- src/tokens/StandardTokenFactory.sol
- src/tokens/DividendDistributor.sol
- src/tokens/BabyTokenDividendTrackerFactory.sol
- src/Configurable.sol
- src/Presale.sol
- src/Recoverable.sol
- src/PresaleFactory.sol
- src/BaseFactory.sol
- src/MultiSender.sol
- src/Operable.sol
- src/Locker.sol
- src/Config.sol
- Toshi-The-Cat/toshi-

solidity/commit/71dbb0b297372b5ce001aaf8c15cdc360e86e9c0

Out-of-Scope: src/mocks/NftMock.sol, src/mocks/TokenMock.sol

REMEDIATION COMMIT ID: ^

- https://github.com/Toshi-The-Cat/toshi-solidity/pull/1/commits/a017976aa1fd88c94d08bf103ca8a962fbbb65be
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/10/commits/4f2891720104 23c9b903c12c0b1ac5061c20db2d
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/2/commits/a7c54bd86c658b8c707351204332ee4dab2c71c9
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/12/commits/ab4fce2f35ebd47a1b39098677d44b9af8c421cb
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/3/commits/e38a45f9a0bf6c075bb1791f4121f02b119cee53
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/4/commits/b6a463eb58dcbd5eb85e1a7124676ad0a6e9440b
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/13/commits/2fca162f1b1c8dadad638f67d5e5716a4d621efa
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/5/commits/2664efe1c7780429587a5e76cb358f9813b70071
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/6/commits/751b195c731ea4a0a521b17f5638ea8fe9fceb6a
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/7/commits/1df904a41a5c82cbca6b4afdbab8ae35eda09131
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/8/commits/7702e3daabcc2d0b3311e2390234c0f881d07cf8
- https://github.com/Toshi-The-Cat/toshi-solidity/pull/9/commits/4538a6c3a477a336ef15e6e6b610e59885a6de2c

Out-of-Scope: New features/implementations after the remediation commit IDs.

4. FINDINGS OVERVIEW

SECURITY ANALYSIS	RISK LEVEL	REMEDIATION
IMPOSSIBILITY TO COLLECT LP FEES FROM LOCKER CONTRACT	CRITICAL	SOLVED - 10/03/2024
OVERRIDEN _UPDATE() FUNCTION SILENTLY BLOCKS DIVIDEND DISTRIBUTION	CRITICAL	SOLVED - 10/03/2024
MISSING QUOTE TOKEN ADDRESS VERIFICATION DENIES LIQUIDITY WITHDRAWAL	HIGH	SOLVED - 10/03/2024
UNSAFE CASTING MAY LEAD TO UNDERFLOW	MEDIUM	SOLVED - 10/03/2024
EXECUTION OF LOCK WITHDRAWAL ON BEHALF OF ANY BENEFICIARY	MEDIUM	SOLVED - 10/03/2024
MISSING ERROR HANDLING IN TRY/CATCH STATEMENTS	MEDIUM	RISK ACCEPTED - 10/03/2024
NO SLIPPAGE PROTECTION ON UNISWAPV2	MEDIUM	RISK ACCEPTED - 10/03/2024

INTERACTIONS		
UNRESTRICTED DEADLINES FOR SWAPS	MEDIUM	RISK ACCEPTED - 10/03/2024
PRECISION LOSS DUE TO DIVISION BEFORE MULTIPLICATION	MEDIUM	SOLVED - 10/03/2024
MISSING IMPLEMENTATION	LOW	RISK ACCEPTED - 10/12/2024
MISSING VALIDATION STEPS ON CONTRACT INITIALIZATION	LOW	RISK ACCEPTED - 10/03/2024
RISK OF CENTRALIZATION IN OPERATOR ROLE MANAGEMENT	LOW	RISK ACCEPTED - 10/03/2024
IMPOSSIBILITY OF CONTRACT INITIALIZATION	LOW	NOT APPLICABLE - 10/03/2024
UNREACHABLE CODE	LOW	SOLVED - 10/03/2024
MISSING FUNCTIONALITY TO REINCLUDE ADDRESS FOR FEES	LOW	RISK ACCEPTED - 10/03/2024
CONTRACT BALANCE		

MANIPULATION CAN TRIGGER UNINTENDED ACTIONS	LOW	RISK ACCEPTED - 10/03/2024	
MISSING EXPLICIT HANDLE FOR POTENTIAL ARITHMETIC ISSUES	LOW	RISK ACCEPTED - 10/03/2024	
PRESALE CAN BE UNEXPECTEDLY CANCELLED INSTEAD OF FINALIZED	LOW	RISK ACCEPTED - 10/03/2024	
INCONSISTENCY BETWEEN NATSPEC AND CODE FOR RATE CALCULATION	LOW	SOLVED - 10/03/2024	
MISSING _DISABLEINITIALIZERS() FUNCTION CALL	LOW	SOLVED - 10/03/2024	
DUPLICATED FUNCTIONALITY	LOW	RISK ACCEPTED - 10/03/2024	
MISSING THRESHOLD VALIDATION IN FEE SETTINGS	LOW	RISK ACCEPTED - 10/03/2024	
MISSING ARRAY LENGTH VALIDATION IN MULTISENDER	LOW	SOLVED - 10/03/2024	
MISSING THRESHOLD			

VERIFICATION FOR DIVIDEND CALCULATION	LOW	RISK ACCEPTED - 10/03/2024	
MISSING THRESHOLD VERIFICATION FOR HODL VALUE	LOW	RISK ACCEPTED - 10/03/2024	
CHECKS EFFECTS INTERACTION PATTERN NOT FOLLOWED	LOW	RISK ACCEPTED - 10/03/2024	
INCORRECT LOGIC FOR CHECKING LIVE PRESALE	LOW	SOLVED - 10/03/2024	
INCONSISTENT MAXBUY AND MINBUY VERIFICATION	LOW	RISK ACCEPTED - 10/03/2024	
POTENTIAL DENIAL OF SERVICE DUE TO UNBOUNDED ARRAY	LOW	RISK ACCEPTED - 10/03/2024	
LIQUIDITY DEPENDENCY	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024	
INCOMPLETE TEST SUITE	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024	
SINGLE STEP OWNERSHIP TRANSFER PROCESS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024	

CENTRALIZATION RISK	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
RISK OF EVM VERSION INCOMPATIBILITY ACROSS CHAINS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
UNINFORMATIVE REVERSALS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
OPEN TO-DO	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
INCOMPLETE NATSPEC DOCUMENTATION	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
IGNORED RETURN VALUES	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
MISSING CHECKS FOR ADDRESS(0)	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
DEPOSITS NOT UPDATED AFTER REFUND	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
COMMENTED LINE OF CODE	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
UNUSED	INFORMATIONAL	ACKNOWLEDGED

FUNCTIONALITY		- 10/13/2024
APPROVALS TO THE ZERO ADDRESS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
MISSING VARIABLE VISIBILITY	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
USE OF MAGIC NUMBERS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
REDUNDANT PAYABLE MODIFIER	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
USE OF LOW LEVEL TRANSFER METHOD	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
FLOATING PRAGMA	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
MISSING EVENTS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
PUBLIC FUNCTIONS NOT CALLED WITHIN CONTRACTS CAN BE MARKED AS EXTERNAL	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
TYPO IN FUNCTION NAME	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024

REDUNDANT CHECKS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
UNOPTIMIZED LOOPS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
STYLE GUIDE OPTIMIZATIONS	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024
ROOM FOR CODE SIMPLIFICATION	INFORMATIONAL	ACKNOWLEDGED - 10/13/2024

Halborn strongly recommends conducting a follow-up assessment of the project either within six months or immediately following any material changes to the codebase, whichever comes first. This approach is crucial for maintaining the project's integrity and addressing potential vulnerabilities introduced by code modifications.