QuillAudits

Audit Report
February, 2022

For

Fananywhere

Contents

Scope of Audit 01

Check Vulnerabilities 01

Techniques and Methods 02

Issue Categories 03

Number of security issues per severity. 03

Introduction 04

A. Contract - FanTokenVesting.sol 05

Low Severity Issues 05

1. Renounce Ownership 05

2. Usage Of block.timestamp 05

B. Contract - FanTokenIssuance.sol 06

Low Severity Issues 06

1. Renounce Ownership 06

2. Payable Functions can lead to unexpected transfers 07

C. Contract - ERC20FanToken.sol 08

Low Severity Issues 08

1. Approve Race 08

Contents

Functional Tests 09

Automated Tests 30

Closing Summary 31

Scope of the Audit

The scope of this audit was to analyze and document the Fananywhere smart contract codebase for quality, security, and correctness.

Checked Vulnerabilities

We have scanned the smart contract for commonly known and more specific vulnerabilities. Here are some of the commonly known vulnerabilities that we considered:

- Re-entrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Use of tx.origin
- Exception disorder
- Gasless send
- Balance equality
- Byte array
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Redundant fallback function
- Send instead of transfer
- Style guide violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level

Techniques and Methods

Throughout the audit of smart contract, care was taken to ensure:

- The overall quality of code.
- Use of best practices.
- Code documentation and comments match logic and expected behaviour.
- Token distribution and calculations are as per the intended behaviour mentioned in the whitepaper.
- Implementation of ERC-20 token standards.
- Efficient use of gas.
- Code is safe from re-entrancy and other vulnerabilities.

The following techniques, methods and tools were used to review all the smart contracts.

Structural Analysis
In this step, we have analysed the design patterns and structure of smart contracts. A thorough check was done to ensure the smart contract is structured in a way that will not result in future problems.

Static Analysis
Static analysis of smart contracts was done to identify contract vulnerabilities. In this step, a series of automated tools are used to test the security of smart contracts.

Code Review / Manual Analysis
Manual analysis or review of code was done to identify new vulnerabilities or verify the vulnerabilities found during the static analysis. Contracts were completely manually analysed, their logic was checked and compared with the one described in the whitepaper. Besides, the results of the automated analysis were manually verified.

Gas Consumption
In this step, we have checked the behaviour of smart contracts in production. Checks were done to know how much gas gets consumed and the possibilities of optimization of code to reduce gas consumption.

Tools and Platforms used for Audit
Remix IDE, Truffle, Truffle Team, Solhint, Mythril, Slither, Solidity statistic analysis, Theo.

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

Risk-level	Description
High	A high severity issue or vulnerability means that your smart contract can be exploited. Issues on this level are critical to the smart contract's performance or functionality, and we recommend these issues be fixed before moving to a live environment.
Medium	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on this level could potentially bring problems, and they should still be fixed.
Low	Low-level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
Informational	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information. There is low-to-no impact.

Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	0	0	0
Acknowledged	0	0	2	0
Closed	0	0	3	0

Introduction

During the period of **November 30, 2021 to February 02, 2022** - QuillAudits Team performed a security audit for Fananywhere smart contracts.

The code for the audit was taken from the following official link: https://gitlab.com/fananywhere/fananywhere-token

V	Date	Commit hash
1	November	955b92a99cc5c6a9254974d5d3d1f63d84dff038
2	February	9d779320809a724ffde75fac6993e5b80a6dbc46

Issues Found – Code Review / Manual Testing

A.Contract - FanTokenVesting.sol

Low severity issues

1. Renounce Ownership

```
contract FanTokenVesting is Ownable {
  using BokkyPooBahsDateTimeLibrary for uint256;
  using SafeERC20 for IERC20;
  using SafeMath for uint256;
```

Description

Typically, the contract's owner is the account that deploys the contract. As a result, the owner is able to perform certain privileged activities on his behalf. The renounceOwnership function is used in smart contracts to renounce ownership. Otherwise, if the contract's ownership has not been transferred previously, it will never have an Owner, which is risky.

Remediation

It is advised that the Owner cannot call renounceOwnership without first transferring ownership to a different address. Additionally, if a multi-signature wallet is utilized, executing the renounceOwnership method for two or more users should be confirmed. Alternatively, the Renounce Ownership functionality can be disabled by overriding it.

Status: Fixed

2. Usage Of block.timestamp

```
function init(uint256 _timestamp) external onlyOwner notInitialized {
        isInitialized = true;
        _initialTimestamp = _timestamp
```

```
uint256 currentTimeStamp = block.timestamp;
        uint256 noOfDays = BokkyPooBahsDateTimeLibrary.diffDays(
            _initialTimestamp,
            currentTimeStamp
        );
```

Description
Block.timestamp is used in the contract. The variable block is a set of variables. The timestamp does not always reflect the current time and may be inaccurate. The value of a block can be influenced by miners. Maximal Extractable Value attacks require a timestamp of up to 900 seconds. There is no guarantee that the value is right, all what is guaranteed is that it is higher than the timestamp of the previous block.

Remediation
You can use an Oracle to get the exact time or verify if a delay of 900 seconds won't destroy the logic of the staking contract.

Status: Acknowledged
The team has acknowledged this issue since timestamp is used here since the issuance happens on a daily basis. Minor time uncertainties are acceptable.

B.Contract - FanTokenIssuance.sol

Low severity issues

1. **Renounce Ownership**

```
contract FanTokenIssuance is Ownable {
  using SafeMath for uint256;
  using SafeERC20 for IERC20;
```

Description
Typically, the contract's owner is the account that deploys the contract. As a result, the owner is able to perform certain privileged activities on his behalf. The renounceOwnership function is used in smart contracts to renounce ownership. Otherwise, if the contract's ownership has not been transferred previously, it will never have an Owner, which is risky.

Remediation
It is advised that the Owner cannot call renounceOwnership without first transferring ownership to a different address. Additionally, if a multi-signature wallet is utilized, executing the renounceOwnership method for two or more users should be confirmed. Alternatively, the Renounce Ownership functionality can be disabled by overriding it.

Status: Fixed

2. Payable Functions can lead to unexpected transfers

```
function withdrawPoolTokens(DistributionType _distributionType)
        public
        payable
        returns (bool withdrawalSuccess)
    {
        uint256 withdrawableAmount = getPoolWithdrawableAmount(
            _distributionType
```

```
  function withdrawTokens() public payable returns (bool withdrawalSuccess) {
        uint256 totalWithdrawableAmount = 0;
```

Description
In the FanTokenIssuance contract, we have two payable functions that doesn't need that the user to make a transfer; thus a user can send by mistake to the contract; thus a user can lose his funds.

Remediation
It is advised if these functions don’t need the payable attribute to remove it.

Status: Fixed

C.Contract - ERC20FanToken.sol

Low severity issues

1. Approve Race

```
function approve(address spender, uint256 amount)
    public
    override(ERC20, IBEP20)
    returns (bool)
{
    return super.approve(spender, amount);
}
```

Description

The standard ERC20 implementation contains a widely-known racing condition in it approve function, wherein a spender is able to witness the token owner broadcast a transaction altering their approval and quickly sign and broadcast a transaction using transferFrom to move the current approved amount from the owner's balance to the spender. If the spender's transaction is validated before the owner's, the spender will be able to get both approval amounts of both transactions.

Remediation

Use increaseAllowance and decreaseAllowance functions to modify the approval amount instead of using the approve function to modify it.

Status: Acknowledged

The team has acknowledged this issue.

Functional Tests

Contract: ERC20FanToken ERC20
✓ should get the deployed contract
✓ should show correct token name and symbol (54ms)
✓ should show correct balance
✓ should show correct Total Supply
✓ should be able to transfer supply to vesting contract (202ms)

Contract: TokenIssuance
✓ should get the deployed contracts
✓ should initialize issuances with correct total token allotments (307ms)
✓ should add token issuances (752ms)
✓ should add beneficiaries to issuance (564ms)
✓ should allow increase and decrease of untouched beneficiary allotments (370ms)
✓ should give proportional pool withdrawable amounts (58ms)
✓ should give the correct total withdrawable amount (211ms)
✓ should allow the beneficiary to withdraw tokens poolwise (487ms)
✓ should allow the beneficiary to withdraw tokens from all pools at once (1588ms)
✓ should allow recovery of excess tokens (516ms)
✓ should allow removal of a new beneficiary (436ms)
✓ should not allow beneficiary allotment to be more than total allotment (580ms)
✓ should not allow decrease or removal of touched beneficiary allotments (250ms)
✓ should not allow removal of a touched beneficiary (179ms)

Contract: TokenIssuance
✓ should get the deployed contracts
✓ should not allow illegal token issuances (633ms)
✓ should not allow illegal beneficiary addition (718ms)
✓ should not allow illegal beneficiary modification (628ms)
✓ should not allow illegal beneficiary removal (571ms)

```
  Contract: FanTokenVesting
    ✓ should get the deployed contracts
    ✓ should show correct total supply (51ms)
    ✓ should allow admin to change the treasury (136ms)
    ✓ should be able to transfer supply to vesting contract (474ms)
    ✓ should return correct initial withdrawable tokens (178ms)
==========================================
********** Checking distribution info *********
==========================================
Setting initialization date: 03/12/2021
  ==> DISTRIBUTION TYPE: TEAM
  ==> TOTAL ALLOTTED TOKENS: 125000000000000000000000000
  ==> TGE TOKENS: 0
  ==> CLIFF PERIOD DAYS: 365
  ==> VESTING PERIOD DAYS: 1461
--
  ==> DISTRIBUTION TYPE: SEED
  ==> TOTAL ALLOTTED TOKENS: 200000000000000000000000000
  ==> TGE TOKENS: 100000000000000000000000
  ==> CLIFF PERIOD DAYS: 31
  ==> VESTING PERIOD DAYS: 365
--
  ==> DISTRIBUTION TYPE: STRATEGIC
  ==> TOTAL ALLOTTED TOKENS: 510000000000000000000000000
  ==> TGE TOKENS: 255000000000000000000000000
  ==> CLIFF PERIOD DAYS: 31
  ==> VESTING PERIOD DAYS: 365
--
  ==> DISTRIBUTION TYPE: PRIVATE1
  ==> TOTAL ALLOTTED TOKENS: 400000000000000000000000000
  ==> TGE TOKENS: 280000000000000000000000000
  ==> CLIFF PERIOD DAYS: 31
  ==> VESTING PERIOD DAYS: 365
--
  ==> DISTRIBUTION TYPE: PRIVATE2
  ==> TOTAL ALLOTTED TOKENS: 660000000000000000000000000
  ==> TGE TOKENS: 528000000000000000000000000
  ==> CLIFF PERIOD DAYS: 31
  ==> VESTING PERIOD DAYS: 365
```

```
--
    1) should set the initial timestamp and vesting days
  ==> DISTRIBUTION TYPE: LIQUIDITY
  ==> TOTAL ALLOTTED TOKENS: 20000000000000000000000000
  ==> TGE TOKENS: 20000000000000000000000000
  ==> CLIFF PERIOD DAYS: 0
  ==> VESTING PERIOD DAYS: 0
--
  ==> DISTRIBUTION TYPE: REWARDS
  ==> TOTAL ALLOTTED TOKENS: 20000000000000000000000000
  ==> TGE TOKENS: 0
  ==> CLIFF PERIOD DAYS: 31
  ==> VESTING PERIOD DAYS: 761
--
  ==> DISTRIBUTION TYPE: MARKETING
  ==> TOTAL ALLOTTED TOKENS: 12000000000000000000000000
  ==> TGE TOKENS: 6000000000000000000000000
  ==> CLIFF PERIOD DAYS: 0
  ==> VESTING PERIOD DAYS: 730
--
  ==> DISTRIBUTION TYPE: RESERVES
  ==> TOTAL ALLOTTED TOKENS: 13500000000000000000000000
  ==> TGE TOKENS: 6750000000000000000000000
  ==> CLIFF PERIOD DAYS: 0
  ==> VESTING PERIOD DAYS: 730
--
    > No events were emitted
    ✓ should not initialize twice (122ms)
=============================================
******* Checking withdrawable schedules *******
=============================================
Shifting from 03/12/2021 to 03/01/2022
  ==> DISTRIBUTION TYPE: TEAM
  ==> INITIALIZED DATE: 03/12/2021
  ==> CHECKING ON: 03/01/2022
  ==> DAYS PASSED: 31
  ==> VESTING MODE: BEFORE CLIFF
```

==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0
--
==> DISTRIBUTION TYPE: SEED
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 100000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 100000000000000000000000
==> CONTRACT RESPONSE: 100000000000000000000000
--
==> DISTRIBUTION TYPE: STRATEGIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 255000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 255000000000000000000000
==> CONTRACT RESPONSE: 255000000000000000000000
--
==> DISTRIBUTION TYPE: PRIVATE1
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 280000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 280000000000000000000000

==> CONTRACT RESPONSE: 280000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE2
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 528000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 528000000000000000000000000
==> CONTRACT RESPONSE: 528000000000000000000000000

--

==> DISTRIBUTION TYPE: PUBLIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 471404958677685950413225
==> INITIAL TOKENS: 460000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 931404958677685950413225
==> CONTRACT RESPONSE: 931404958677685950413225

--

==> DISTRIBUTION TYPE: ADVISORS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0

--

==> DISTRIBUTION TYPE: LIQUIDITY
==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 200000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000000
--
==> DISTRIBUTION TYPE: REWARDS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0
--
==> DISTRIBUTION TYPE: MARKETING
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 484109589041095890410958
==> INITIAL TOKENS: 600000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 108410958904109589041095
==> CONTRACT RESPONSE: 108410958904109589041095
--
==> DISTRIBUTION TYPE: RESERVES
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 54462328767123287671232

==> INITIAL TOKENS: 675000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 121962328767123287671232 83
==> CONTRACT RESPONSE: 121962328767123287671232 83

--

==> DISTRIBUTION TYPE: ECOSYSTEM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2022
==> DAYS PASSED: 31
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0

--

Shifting from 03/01/2022 to 03/02/2022
==> DISTRIBUTION TYPE: TEAM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0

--

==> DISTRIBUTION TYPE: SEED
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 32273972602739726027396 98
==> INITIAL TOKENS: 100000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 42273972602739726027396 98

==> CONTRACT RESPONSE: 42273972602739726027396 98

--

==> DISTRIBUTION TYPE: STRATEGIC

==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/02/2022

==> DAYS PASSED: 62

==> VESTING MODE: PARTIAL VESTED

==> VESTED AMOUNT: 822986301369863013698 6264

==> INITIAL TOKENS: 25500000000000000000000000

==> WITHDRAWN TOKENS: 0

==> UNLOCKED TOKENS: 107798630136986301369 86264

==> CONTRACT RESPONSE: 107798630136986301369 86264

--

==> DISTRIBUTION TYPE: PRIVATE1

==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/02/2022

==> DAYS PASSED: 62

==> VESTING MODE: PARTIAL VESTED

==> VESTED AMOUNT: 631890410958904109589 0360

==> INITIAL TOKENS: 28000000000000000000000000

==> WITHDRAWN TOKENS: 0

==> UNLOCKED TOKENS: 911890410958904109589 0360

==> CONTRACT RESPONSE: 911890410958904109589 0360

--

==> DISTRIBUTION TYPE: PRIVATE2

==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/02/2022

==> DAYS PASSED: 62

==> VESTING MODE: PARTIAL VESTED

==> VESTED AMOUNT: 103140821917808219178 08192

==> INITIAL TOKENS: 52800000000000000000000000

==> WITHDRAWN TOKENS: 0

==> UNLOCKED TOKENS: 155940821917808219178 08192

==> CONTRACT RESPONSE: 155940821917808219178 08192

--

==> DISTRIBUTION TYPE: PUBLIC

==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 942809917355371900826445O
==> INITIAL TOKENS: 460000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 140280991735537190082644SO
==> CONTRACT RESPONSE: 140280991735537190082644SO
--
==> DISTRIBUTION TYPE: ADVISORS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0
--
==> DISTRIBUTION TYPE: LIQUIDITY
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 200000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000
--
==> DISTRIBUTION TYPE: REWARDS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 162943495400788436268067SO

==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 162943495400788436268067 98
==> CONTRACT RESPONSE: 162943495400788436268067 98

--

==> DISTRIBUTION TYPE: MARKETING
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 96821917808219178082191 56
==> INITIAL TOKENS: 600000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 156821917808219178082191 56
==> CONTRACT RESPONSE: 156821917808219178082191 56

--

==> DISTRIBUTION TYPE: RESERVES
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 10892465753424657534246566
==> INITIAL TOKENS: 675000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 176424657534246575342465 66
==> CONTRACT RESPONSE: 176424657534246575342465 66

--

==> DISTRIBUTION TYPE: ECOSYSTEM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/02/2022
==> DAYS PASSED: 62
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 139688041594454072790294 42
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 139688041594454072790294 42
==> CONTRACT RESPONSE: 139688041594454072790294 42

--
Shifting from 03/02/2022 to 03/12/2022
==> DISTRIBUTION TYPE: TEAM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: BEFORE CLIFF
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 0
==> CONTRACT RESPONSE: 0
--
==> DISTRIBUTION TYPE: SEED
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 190000000000000000000000000
==> INITIAL TOKENS: 100000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000000
--
==> DISTRIBUTION TYPE: STRATEGIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 484500000000000000000000000
==> INITIAL TOKENS: 255000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 510000000000000000000000000
==> CONTRACT RESPONSE: 510000000000000000000000000
--
==> DISTRIBUTION TYPE: PRIVATE1
==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 372000000000000000000000000
==> INITIAL TOKENS: 280000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 400000000000000000000000000
==> CONTRACT RESPONSE: 400000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE2
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 607200000000000000000000000
==> INITIAL TOKENS: 528000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 660000000000000000000000000
==> CONTRACT RESPONSE: 660000000000000000000000000

--

==> DISTRIBUTION TYPE: PUBLIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 184000000000000000000000000
==> INITIAL TOKENS: 460000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 230000000000000000000000000
==> CONTRACT RESPONSE: 230000000000000000000000000

--

==> DISTRIBUTION TYPE: ADVISORS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 349999999999999999999965

==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 349999999999999999999965
==> CONTRACT RESPONSE: 349999999999999999999965
--
==> DISTRIBUTION TYPE: LIQUIDITY
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 200000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000000
--
==> DISTRIBUTION TYPE: REWARDS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 959264126149802890932980 85
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 959264126149802890932980 85
==> CONTRACT RESPONSE: 959264126149802890932980 85
--
==> DISTRIBUTION TYPE: MARKETING
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 569999999999999999999870
==> INITIAL TOKENS: 600000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 629999999999999999999870
==> CONTRACT RESPONSE: 629999999999999999999870

--
==> DISTRIBUTION TYPE: RESERVES
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 641249999999999999999945
==> INITIAL TOKENS: 675000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 708749999999999999999945
==> CONTRACT RESPONSE: 708749999999999999999945
--
==> DISTRIBUTION TYPE: ECOSYSTEM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/12/2022
==> DAYS PASSED: 365
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 82235701906412478336221715
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 82235701906412478336221715
==> CONTRACT RESPONSE: 82235701906412478336221715
--
Shifting from 03/12/2022 to 03/01/2023
==> DISTRIBUTION TYPE: TEAM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 338809034907597535934289l2
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 338809034907597535934289l2
==> CONTRACT RESPONSE: 338809034907597535934289l2
--
==> DISTRIBUTION TYPE: SEED
==> INITIALIZED DATE: 03/12/2021

==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 190000000000000000000000000
==> INITIAL TOKENS: 100000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000000

--

==> DISTRIBUTION TYPE: STRATEGIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 484500000000000000000000000
==> INITIAL TOKENS: 255000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 510000000000000000000000000
==> CONTRACT RESPONSE: 510000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE1
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 372000000000000000000000000
==> INITIAL TOKENS: 280000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 400000000000000000000000000
==> CONTRACT RESPONSE: 400000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE2
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 607200000000000000000000000

==> INITIAL TOKENS: 528000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 660000000000000000000000000
==> CONTRACT RESPONSE: 660000000000000000000000000

--

==> DISTRIBUTION TYPE: PUBLIC
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 184000000000000000000000000
==> INITIAL TOKENS: 460000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 230000000000000000000000000
==> CONTRACT RESPONSE: 230000000000000000000000000

--

==> DISTRIBUTION TYPE: ADVISORS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 379726027397260273972602 36
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 379726027397260273972602 36
==> CONTRACT RESPONSE: 379726027397260273972602 36

--

==> DISTRIBUTION TYPE: LIQUIDITY
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: TOTAL VESTED
==> VESTED AMOUNT: 0
==> INITIAL TOKENS: 200000000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 200000000000000000000000000
==> CONTRACT RESPONSE: 200000000000000000000000000

--

==> DISTRIBUTION TYPE: REWARDS
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 104073587385019710906701484
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 104073587385019710906701484
==> CONTRACT RESPONSE: 104073587385019710906701484

--

==> DISTRIBUTION TYPE: MARKETING
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 61841095890410958904109448
==> INITIAL TOKENS: 600000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 67841095890410958904109448
==> CONTRACT RESPONSE: 67841095890410958904109448

--

==> DISTRIBUTION TYPE: RESERVES
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023
==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 695712328767123287671232 28
==> INITIAL TOKENS: 675000000000000000000000
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 763212328767123287671232 28
==> CONTRACT RESPONSE: 763212328767123287671232 28

--

==> DISTRIBUTION TYPE: ECOSYSTEM
==> INITIALIZED DATE: 03/12/2021
==> CHECKING ON: 03/01/2023

==> DAYS PASSED: 396
==> VESTING MODE: PARTIAL VESTED
==> VESTED AMOUNT: 892201039861351819757364 36
==> INITIAL TOKENS: 0
==> WITHDRAWN TOKENS: 0
==> UNLOCKED TOKENS: 892201039861351819757364 36
==> CONTRACT RESPONSE: 892201039861351819757364 36
--
✓ should check withdrawable tokens for various elapsed times (3312ms)

Contract: FanTokenVesting
✓ should get the deployed contracts
✓ should be able to some tokens to vesting contract (142ms)
✓ should throw on initializing with insufficient funds (2436ms)
✓ should throw on calling `initialized` methods (190ms)
✓ should throw on calling `onlyOwner` methods with non-owner account (422ms)

Contract: FanTokenVesting
✓ should get the deployed contracts
==========
********* Checking vesting withdrawals *********
==========
Vesting contract initialized At: 03/12/2021
Shifting from 03/12/2021 to 03/12/2025
==> DISTRIBUTION TYPE: TEAM
==> BEFORE WITHDRAW
- UNLOCKED TOKENS: 125000000000000000000000000
- CONTRACT BALANCE: 1000000000000000000000000000
- TREASURY BALANCE: 0
==> AFTER WITHDRAW
- UNLOCKED : 0
- CONTRACT BALANCE: 875000000000000000000000000
- TREASURY BALANCE: 125000000000000000000000000
--
==> DISTRIBUTION TYPE: SEED

==> BEFORE WITHDRAW
- UNLOCKED TOKENS: 200000000000000000000000000
- CONTRACT BALANCE: 875000000000000000000000000
- TREASURY BALANCE: 125000000000000000000000000

==> AFTER WITHDRAW
- UNLOCKED : 0
- CONTRACT BALANCE: 855000000000000000000000000
- TREASURY BALANCE: 145000000000000000000000000

--

==> DISTRIBUTION TYPE: STRATEGIC
==> BEFORE WITHDRAW
- UNLOCKED TOKENS: 510000000000000000000000000
- CONTRACT BALANCE: 855000000000000000000000000
- TREASURY BALANCE: 145000000000000000000000000

==> AFTER WITHDRAW
- UNLOCKED : 0
- CONTRACT BALANCE: 804000000000000000000000000
- TREASURY BALANCE: 196000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE1
==> BEFORE WITHDRAW
- UNLOCKED TOKENS: 400000000000000000000000000
- CONTRACT BALANCE: 804000000000000000000000000
- TREASURY BALANCE: 196000000000000000000000000

==> AFTER WITHDRAW
- UNLOCKED : 0
- CONTRACT BALANCE: 764000000000000000000000000
- TREASURY BALANCE: 236000000000000000000000000

--

==> DISTRIBUTION TYPE: PRIVATE2
==> BEFORE WITHDRAW
- UNLOCKED TOKENS: 660000000000000000000000000
- CONTRACT BALANCE: 764000000000000000000000000
- TREASURY BALANCE: 236000000000000000000000000

==> AFTER WITHDRAW
- UNLOCKED : 0
- CONTRACT BALANCE: 698000000000000000000000000
- TREASURY BALANCE: 302000000000000000000000000

```
--
  ==> DISTRIBUTION TYPE: PUBLIC
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 230000000000000000000000000
        - CONTRACT BALANCE: 698000000000000000000000000
        - TREASURY BALANCE: 302000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 675000000000000000000000000
        - TREASURY BALANCE: 325000000000000000000000000
--
  ==> DISTRIBUTION TYPE: ADVISORS
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 700000000000000000000000000
        - CONTRACT BALANCE: 675000000000000000000000000
        - TREASURY BALANCE: 325000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 605000000000000000000000000
        - TREASURY BALANCE: 395000000000000000000000000
--
  ==> DISTRIBUTION TYPE: LIQUIDITY
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 200000000000000000000000000
        - CONTRACT BALANCE: 605000000000000000000000000
        - TREASURY BALANCE: 395000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 585000000000000000000000000
        - TREASURY BALANCE: 415000000000000000000000000
--
  ==> DISTRIBUTION TYPE: REWARDS
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 200000000000000000000000000
        - CONTRACT BALANCE: 585000000000000000000000000
        - TREASURY BALANCE: 415000000000000000000000000
  ==> AFTER WITHDRAW
```

```
        - UNLOCKED : 0
        - CONTRACT BALANCE: 385000000000000000000000000
        - TREASURY BALANCE: 615000000000000000000000000
--
  ==> DISTRIBUTION TYPE: MARKETING
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 120000000000000000000000000
        - CONTRACT BALANCE: 385000000000000000000000000
        - TREASURY BALANCE: 615000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 265000000000000000000000000
        - TREASURY BALANCE: 735000000000000000000000000
--
  ==> DISTRIBUTION TYPE: RESERVES
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 135000000000000000000000000
        - CONTRACT BALANCE: 265000000000000000000000000
        - TREASURY BALANCE: 735000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 130000000000000000000000000
        - TREASURY BALANCE: 870000000000000000000000000
--
  ==> DISTRIBUTION TYPE: ECOSYSTEM
  ==> BEFORE WITHDRAW
        - UNLOCKED TOKENS: 130000000000000000000000000
        - CONTRACT BALANCE: 130000000000000000000000000
        - TREASURY BALANCE: 870000000000000000000000000
  ==> AFTER WITHDRAW
        - UNLOCKED : 0
        - CONTRACT BALANCE: 0
        - TREASURY BALANCE: 1000000000000000000000000000
--
    ✓ should be able to withdraw tokens and reduce contracts balance
(9167ms)
    ✓ should allow admin to recover excess tokens (611ms)

  40 passing (43s)
```

Automated Tests

Slither

```
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (ERC20FanToken.sol#287) necessitates a version too recent t
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (ERC20FanToken.sol#317) necessitates a version too recent t
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (ERC20FanToken.sol#344) necessitates a version too recent t
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (ERC20FanToken.sol#702) necessitates a version too recent t
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version0.8.9 (ERC20FanToken.sol#746) necessitates a version too recent to
 be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (ERC20FanToken.sol#834) necessitates a version too recent t
o be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version0.8.9 (ERC20FanToken.sol#911) necessitates a version too recent to
 be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.9 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorre
ct-versions-of-solidity

Variable ERC20Permit.DOMAIN_SEPARATOR (ERC20FanToken.sol#760) is not in mixedCas
e
Parameter ERC20FanToken.allowance(address,address)._owner (ERC20FanToken.sol#100
4) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conform
ance-to-solidity-naming-conventions

ERC20FanToken.slitherConstructorConstantVariables() (ERC20FanToken.sol#919-1028)
 uses literals with too many digits:
        - MAX_CAP = 1000000000 * (10 ** 18) (ERC20FanToken.sol#920)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-man
y-digits

ERC20FanToken (ERC20FanToken.sol#919-1028) does not implement functions:
        - IBEP20.allowance(address,address) (ERC20FanToken.sol#57-60)
        - IBEP20.approve(address,uint256) (ERC20FanToken.sol#76)
        - IBEP20.balanceOf(address) (ERC20FanToken.sol#37)
        - IBEP20.decimals() (ERC20FanToken.sol#17)
        - IBEP20.symbol() (ERC20FanToken.sol#22)
        - IBEP20.totalSupply() (ERC20FanToken.sol#12)
        - IBEP20.transfer(address,uint256) (ERC20FanToken.sol#46-48)
        - IBEP20.transferFrom(address,address,uint256) (ERC20FanToken.sol#87-91)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimple
mented-functions

increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (ERC20FanToken.sol#517-520)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (ERC20FanToken.sol#536-544)
permit(address,address,uint256,uint256,uint8,bytes32,bytes32) should be declared
 external:
        - ERC20Permit.permit(address,address,uint256,uint256,uint8,bytes32,bytes
32) (ERC20FanToken.sol#785-819)
nonces(address) should be declared external:
        - ERC20Permit.nonces(address) (ERC20FanToken.sol#824-826)
renounceOwnership() should be declared external:
        - ERC20FanToken.renounceOwnership() (ERC20FanToken.sol#983-985)
        - Ownable.renounceOwnership() (ERC20FanToken.sol#883-885)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (ERC20FanToken.sol#891-894)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-
function-that-could-be-declared-external
ERC20FanToken.sol analyzed (11 contracts with 75 detectors), 30 result(s) found
```

Results

No major issues were found. Some false positive errors were reported by the tool. All the other issues have been categorized above according to their level of severity.

Closing Summary

Overall, smart contracts are very well written and adhere to guidelines.

No instances of Integer Overflow and Underflow vulnerabilities or Back-Door Entry were found in the contract; All the issues found were Fixed or acknowledged by the Fananywhere team.

Disclaimer

Quillhash audit is not a security warranty, investment advice, or an endorsement of the Fananywhere Contract. This audit does not provide a security or correctness guarantee of the audited smart contracts. The statements made in this document should not be interpreted as investment or legal advice, nor should its authors be held accountable for decisions made based on them. Securing smart contracts is a multistep process. One audit cannot be considered enough. We recommend that the Fananywhere Team put in place a bug bounty program to encourage further analysis of the smart contract by other third parties.

Audit Report
February, 2022

For

Fananywhere

QuillAudits

Canada, India, Singapore, United Kingdom

audits.quillhash.com

audits@quillhash.com