



# FLIGHT CLUP COIN Smart Contract Audit Report

# TABLE OF CONTENTS

## [Audited Details](#)

- Audited Project
- Blockchain
- Addresses
- Project Website
- Codebase

## [Summary](#)

- Contract Summary
- Audit Findings Summary
- Vulnerabilities Summary

## [Conclusion](#)

## [Audit Results](#)

## [Smart Contract Analysis](#)

- Detected Vulnerabilities

## [Disclaimer](#)

## [About Us](#)

# AUDITED DETAILS

## Audited Project

Project name	Token ticker	Blockchain
FLIGHT CLUP COIN	FLIGHT	Binance Smart Chain

## Addresses

Contract address	0xf397680d99a92e4b60637e9f5c71a4def1f6c7b5
Contract deployer address	0xe36084e81fCCCfc36828F8E3E36DF38b7326D3E9

## Project Website

<a href="https://www.flightclupcoin.com/">https://www.flightclupcoin.com/</a>
---

## Codebase

<a href="https://bscscan.com/address/0xf397680d99a92e4b60637e9f5c71a4def1f6c7b5#code">https://bscscan.com/address/0xf397680d99a92e4b60637e9f5c71a4def1f6c7b5#code</a>
---

# SUMMARY

Flight Club is a decentralized community led by elite cryptocurrency and blockchain experts. All Flight Club members have equal opportunities. Flight Club allows all its members to establish their businesses registered in the blockchain system, and at the same time, each member is a club shareholder. The club belongs to the members. This approach, which is unique in the world, is the advanced version of the idea that puts freedom and people in the center, where Satoshi Nakamoto, the architect of BITCOIN, left off. All Flight Club members feed and support each other; the rise of a member does not disturb another member; on the contrary, it makes them happy because the rising member causes others to win. Flight Club, which has a unique ecosystem, is a public, blockchain-based platform equipped with the highest technology that anyone who wants to change their life can benefit from.

## Contract Summary

### Documentation Quality

FLIGHT CLUP COIN provides a very poor documentation with standard of solidity base code.

- The technical description is provided unclear and disorganized.

### Code Quality

The Overall quality of the basecode is poor.

- Solidity basecode and rules are unclear and disorganized by FLIGHT CLUP COIN.

### Test Coverage

Test coverage of the project is 100% ( Through Codebase )

## Audit Findings Summary

- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 297 and 298.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 9.
- SWC-110 SWC-123 | It is recommended to use of revert(), assert(), and require() in Solidity, and the new REVERT opcode in the EVM on lines 159.

## CONCLUSION

We have audited the FLIGHT CLUP COIN project released on September 2022 to find issues and identify potential security vulnerabilities in the FLIGHT CLUP COIN project. This process is used to find technical issues and security loopholes that may be found in smart contracts.

The security audit report yielded unsatisfactory results, discovering high-risk and low-risk issues.

Writing a contract that does not follow the Solidity style guide can pose a significant risk. The serious and low problems we found in the smart contract are the arithmetic operation can overflow. It is possible to cause an arithmetic overflow. Prevent the overflow by constraining inputs using the `require()` statement or the OpenZeppelin SafeMath library for integer arithmetic operations. Refer to the transaction trace generated for this issue to reproduce the overflow. Low-risk issue the arithmetic operation can overflow and cause requirement violation. The current pragma Solidity directive is `">=0.4.220.6.0"`. Specifying a fixed compiler version is recommended to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code. A requirement was violated in a nested call, and the call was reverted. Ensure valid inputs are provided to the nested call (for instance, via passed arguments).

We were recommended to keep being aware of investing in this risky smart contract.

# AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	PASS
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	ISSUE FOUND
Unchecked Call Return Value	SWC-104	The return value of a message call should be checked.	PASS
Unprotected Ether Withdrawal	SWC-105	Due to missing or insufficient access controls, malicious parties can withdraw from the contract.	PASS
SELFDESTRUCT Instruction	SWC-106	The contract should not be self-destructible while it has funds belonging to users.	PASS
Reentrancy	SWC-107	Check effect interaction pattern should be followed if the code performs recursive call.	PASS
Uninitialized Storage Pointer	SWC-109	Uninitialized local storage variables can point to unexpected storage locations in the contract.	PASS
Assert Violation	SWC-110 SWC-123	Properly functioning code should never reach a failing assert statement.	ISSUE FOUND
Deprecated Solidity Functions	SWC-111	Deprecated built-in functions should never be used.	PASS
Delegate call to Untrusted Callee	SWC-112	Delegatecalls should only be allowed to trusted addresses.	PASS

DoS (Denial of Service)	<b>SWC-113</b> <b>SWC-128</b>	Execution of the code should never be blocked by a specific contract state unless required.	<b>PASS</b>
Race Conditions	<b>SWC-114</b>	Race Conditions and Transactions Order Dependency should not be possible.	<b>PASS</b>
Authorization through tx.origin	<b>SWC-115</b>	tx.origin should not be used for authorization.	<b>PASS</b>
Block values as a proxy for time	<b>SWC-116</b>	Block numbers should not be used for time calculations.	<b>PASS</b>
Signature Unique ID	<b>SWC-117</b> <b>SWC-121</b> <b>SWC-122</b>	Signed messages should always have a unique id. A transaction hash should not be used as a unique id.	<b>PASS</b>
Incorrect Constructor Name	<b>SWC-118</b>	Constructors are special functions that are called only once during the contract creation.	<b>PASS</b>
Shadowing State Variable	<b>SWC-119</b>	State variables should not be shadowed.	<b>PASS</b>
Weak Sources of Randomness	<b>SWC-120</b>	Random values should never be generated from Chain Attributes or be predictable.	<b>PASS</b>
Write to Arbitrary Storage Location	<b>SWC-124</b>	The contract is responsible for ensuring that only authorized user or contract accounts may write to sensitive storage locations.	<b>PASS</b>
Incorrect Inheritance Order	<b>SWC-125</b>	When inheriting multiple contracts, especially if they have identical functions, a developer should carefully specify inheritance in the correct order. The rule of thumb is to inherit contracts from more /general/ to more /specific/.	<b>PASS</b>
Insufficient Gas Griefing	<b>SWC-126</b>	Insufficient gas grieving attacks can be performed on contracts which accept data and use it in a sub-call on another contract.	<b>PASS</b>
Arbitrary Jump Function	<b>SWC-127</b>	As Solidity doesnt support pointer arithmetics, it is impossible to change such variable to an arbitrary value.	<b>PASS</b>

Typographical Error	<b>SWC-129</b>	A typographical error can occur for example when the intent of a defined operation is to sum a number to a variable.	<b>PASS</b>
Override control character	<b>SWC-130</b>	Malicious actors can use the Right-To-Left-Override unicode character to force RTL text rendering and confuse users as to the real intent of a contract.	<b>PASS</b>
Unused variables	<b>SWC-131</b> <b>SWC-135</b>	Unused variables are allowed in Solidity and they do not pose a direct security issue.	<b>PASS</b>
Unexpected Ether balance	<b>SWC-132</b>	Contracts can behave erroneously when they strictly assume a specific Ether balance.	<b>PASS</b>
Hash Collisions Variable	<b>SWC-133</b>	Using <code>abi.encodePacked()</code> with multiple variable length arguments can, in certain situations, lead to a hash collision.	<b>PASS</b>
Hardcoded gas amount	<b>SWC-134</b>	The <code>transfer()</code> and <code>send()</code> functions forward a fixed amount of 2300 gas.	<b>PASS</b>
Unencrypted Private Data	<b>SWC-136</b>	It is a common misconception that private type variables cannot be read.	<b>PASS</b>



# SMART CONTRACT ANALYSIS

Started	Thursday Sep 15 2022 04:30:27 GMT+0000 (Coordinated Universal Time)
Finished	Friday Sep 16 2022 14:24:23 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	TradeToken.sol

## | Detected Issues

ID	Title	Severity	Status
SWC-101	THE ARITHMETIC OPERATION CAN OVERFLOW.	high	acknowledged
SWC-101	THE ARITHMETIC OPERATION CAN OVERFLOW.	high	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-123	REQUIREMENT VIOLATION.	low	acknowledged

# SWC-101 | THE ARITHMETIC OPERATION CAN OVERFLOW.

LINE 297

## high SEVERITY

It is possible to cause an arithmetic overflow. Prevent the overflow by constraining inputs using the require() statement or use the OpenZeppelin SafeMath library for integer arithmetic operations. Refer to the transaction trace generated for this issue to reproduce the overflow.

## Source File

- TradeToken.sol

## Locations

```

296  if (isHolder[target] != true) {                                // ??? ? ????????? ????
??????? ? ??????
297  holders[holders.length++] = target;                            // ??? ? ????????? ???? ??
?????, ???????? ??? ????????? ????????? ?????.
298  isHolder[target] = true;
299  }
300
301
    
```

# SWC-101 | THE ARITHMETIC OPERATION CAN OVERFLOW.

LINE 298

## high SEVERITY

It is possible to cause an arithmetic overflow. Prevent the overflow by constraining inputs using the require() statement or use the OpenZeppelin SafeMath library for integer arithmetic operations. Refer to the transaction trace generated for this issue to reproduce the overflow.

## Source File

- TradeToken.sol

## Locations

```

297  holders[holders.length++] = target;                // ??? ???? ???? ?
????, ????? ? ? ???? ???? ???? ? ? ?????.
298  isHolder[target] = true;
299  }
300
301  emit Transfer(address(0), address(this), mintedAmount);
302
    
```

## SWC-103 | A FLOATING PRAGMA IS SET.

LINE 9

### low SEVERITY

The current pragma Solidity directive is `">=0.4.22<0.6.0"`. It is recommended to specify a fixed compiler version to ensure that the bytecode produced does not vary between builds. This is especially important if you rely on bytecode-level verification of the code.

### Source File

- TradeToken.sol

### Locations

```
8
9  pragma solidity >=0.4.22 <0.6.0;
10
11  contract owned {
12      address public owner;
13  }
```

## SWC-123 | REQUIREMENT VIOLATION.

LINE 159

### low SEVERITY

A requirement was violated in a nested call and the call was reverted as a result. Make sure valid inputs are provided to the nested call (for instance, via passed arguments).

### Source File

- TradeToken.sol

### Locations

```
158 spender.receiveApproval(msg.sender, _value, address(this), _extraData);
159 return true;
160 }
161 }
162
163
```

# 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 you ("Customer" or 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, nor may copies be delivered to any other person other than the Company, without Sysfixed's prior written consent in each instance.

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 Sysfixed 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 is a limited report on our findings based on our analysis, in accordance with good industry practice as of the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

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.

This report is provided for information purposes only and on a non-reliance basis and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and Sysfixed and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers, and other representatives) (Sysfixed) owe no duty of care.

## ABOUT US

Sysfixed is a blockchain security certification organization established in 2021 with the objective to provide smart contract security services and verify their correctness in blockchain-based protocols. Sysfixed automatically scans for security vulnerabilities in Ethereum and other EVM-based blockchain smart contracts. Sysfixed a comprehensive range of analysis techniques—including static analysis, dynamic analysis, and symbolic execution—can accurately detect security vulnerabilities to provide an in-depth analysis report. With a vibrant ecosystem of world-class integration partners that amplify developer productivity, Sysfixed can be utilized in all phases of your project's lifecycle. Our team of security experts is dedicated to the research and improvement of our tools and techniques used to fortify your code.