CFG NINJA AUDITS

Security Assessment

Sports Future

Exchange Token Token

November 26, 2023

Audit Status: Pass

Audit Edition: Standard

SPOFU**X**

Risk Analysis

Classifications of Manual Risk Results

Classification	Description
🔴 Critical	Danger or Potential Problems.
🟠 High	Be Careful or Fail test.
🟢 Low	Pass, Not-Detected or Safe Item.
🔵 Informational	Function Detected

Manual Code Review Risk Results

Contract Priviledge	Description
🟢 Buy Tax	12%
🟢 Sale Tax	12%
🟢 Cannot Sale	Pass
🟢 Cannot Sale	Pass
🟢 Max Tax	12%
🟢 Modify Tax	Yes
🟢 Fee Check	Pass
🟢 Is Honeypot?	Not Detected
🟢 Trading Cooldown	Not Detected
🔴 Can Pause Trade?	Fail

Contract Priviledge	Description
🔴 Pause Transfer?	Detected, Owner need to enable trade.
🟢 Max Tx?	Pass
🟢 Is Anti Whale?	Not Detected
🟢 Is Anti Bot?	Not Detected
🟢 Is Blacklist?	Not Detected
🟢 Blacklist Check	Pass
🟡 is Whitelist?	Detected
🟢 Can Mint?	Pass
🟢 Is Proxy?	Not Detected
🟢 Can Take Ownership?	Not Detected
🟢 Hidden Owner?	Not Detected
🔵 Owner	0xa101ed9019948ec99Dc5272fc9e90Dcb752Eb41e
🟢 Self Destruct?	Not Detected
🟢 External Call?	Not Detected
🟢 Other?	Not Detected
🟢 Holders	1
🔴 Auditor Confidence	Low
🟢 KYC Completed	Yes

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Project Overview

Token Summary

Parameter	Result
Address	0xd8C9091a2Bd78477bFeE618EAB5864715e405513
Name	Sports Future Exchange Token
Token Tracker	Sports Future Exchange Token (Spox)
Decimals	18
Supply	100,000,000,000
Platform	Binance Smart Chain
compiler	v0.8.9+commit.e5eed63a
Contract Name	Spox
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://bscscan.com/token/0xd8C9091a2Bd78477bFeE618EAB5864715e405513#code
Payment Tx	Corporate

Project Overview

Simulation Summary

Parameter	Result
Transfer From Owner	Pass
Transfer From Holder	Pass
Add Liquidity	Pass
RemoveLiquidity	Pass
Buy from Owner	Pass
Buy from Holder	Pass
Sale from Owner	Pass
Sale from Holder	Pass
Remove Liquidity	Pass
SwapAndLiquify	Pass
SwapAndSale w/Fee	Pass
SwapAndSale TX	https://testnet.bscscan.com/tx/0xba09eb98251920b3180c8bb29e3216ece1210c0d63c29cd899acec5141e2f9c4
SwapAndSaleNoFee	Pass
SwapAndSale No/Fee TX	https://testnet.bscscan.com/tx/0x4ee0e7af62eb27553310c7deaa33b4e91c7abb22f1b3fca85dc0c4bfeb6f4867

Parameter	Result
ExcludeFromFees	Pass
LaunchPad	PinkSale
Pool Creation	N/A
Pool Creation TX	
Pool Finalize	N/A
Pool Finalize TX	
Enable	Pass, https://testnet.bscscan.com/tx/0x 0697b0c1ced17c040600cab96fc2c37b1 2b5184d563a0016cf96ccf6f003f613

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Main Contract Assessed
Contract Name

Name	Contract	Live
Sports Future Exchange Token	0xd8C9091a2Bd78477bFeE618EAB5864715e405513	Yes

TestNet Contract Assessed
Contract Name

Name	Contract	Live
Sports Future Exchange Token	0x6d38FD50D519b26eF00B011Adb7938A0227DF122	Yes

Solidity Code Provided

SolID	File Sha-1	FileName
Sporx	ac405da9976ce1826fe7c016cc4f49abb4f311d2	Sporx.sol

Call Graph

The contract for Sports Future Exchange Token has the following call graph structure.
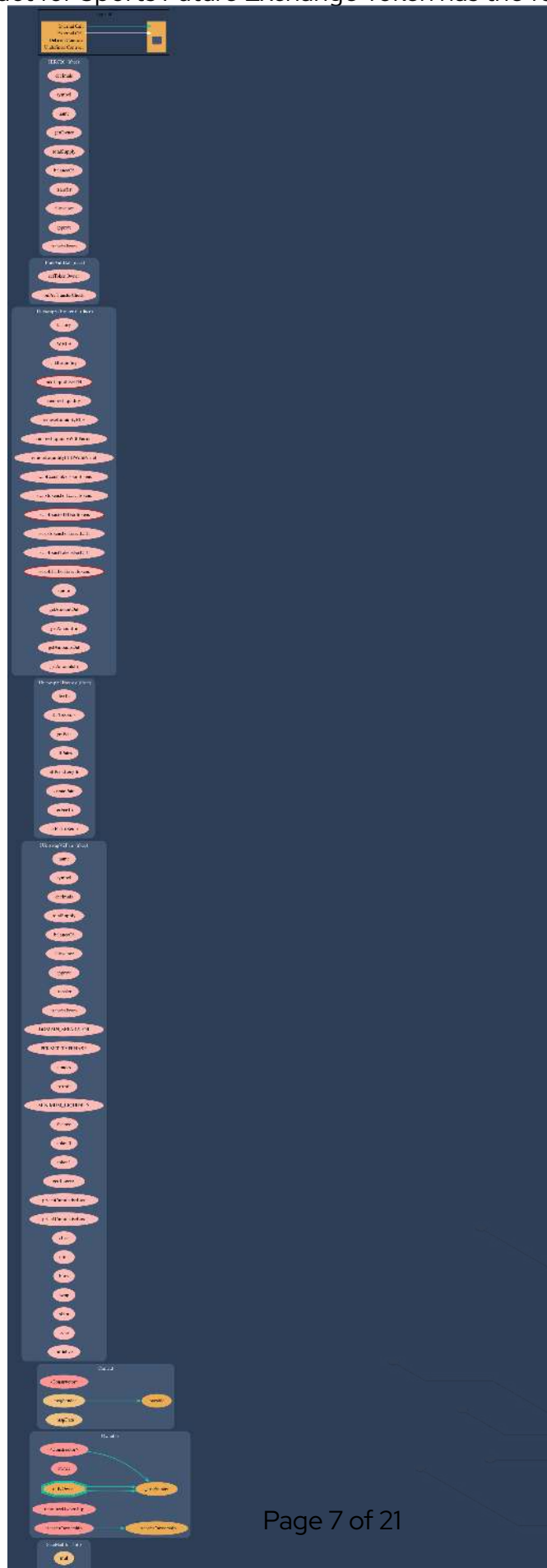
Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	Sporx.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	Sporx.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	Sporx.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	Sporx.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	Sporx.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	Sporx.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	Sporx.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	Sporx.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	Sporx.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	Sporx.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	Sporx.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-111	Pass	Use of Deprecated Solidity Functions.	Sporx.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	Sporx.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	Sporx.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	Sporx.sol	L: 0 C: 0
SWC-115	Pass	Authorization through tx.origin.	Sporx.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	Sporx.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	Sporx.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	Sporx.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	Sporx.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	Sporx.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	Sporx.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	Sporx.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	Sporx.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	Sporx.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	Sporx.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-126	Pass	Insufficient Gas Griefing.	Sporx.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	Sporx.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	Sporx.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	Sporx.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	Sporx.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	Sporx.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	Sporx.sol	L: 0 C: 0
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	Sporx.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	Sporx.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	Sporx.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	Sporx.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Inheritance

The contract for Sports Future Exchange Token has the following inheritance structure.

Spox-03 | Lack of Input Validation.

Category	Severity	Location	Status
Volatile Code	🟢 Low	Sporx.sol: L: 304 C: 14, L: 300 2C: 14, L: 296 2C: 14, L: 292 2C: 14, L: 268 2C: 14, L: 253 2C: 14, L: 240 2C: 14, L: 235 2C: 14	🗒️Detected

Description

The given input is missing the check for the non-zero address.

The given input is missing the check for the all onlyOwner..

Recommendation

We advise the client to add the check for the passed-in values to prevent unexpected errors as below:
```
    ...
     require(receiver != address(0), "Receiver is the zero address");
    ...
    ...
    require(value X limitation, "Your not able to do this function");
    ...
```

We also recommend customer to review the following function that is missing a required validation. all onlyOwner..

Mitigation

undefined

References:

Zero Address check. The danger!!!

Spox-05 | Missing Event Emission.

Category	Severity	Location	Status
Volatile Code	🟢 Low	Sporx.sol: L: 304 C: 14, L: 300 2C: 14, L: 296 2C: 14, L: 292 2C: 14, L: 268 2C: 14, L: 253 2C: 14, L: 240 2C: 14, L: 235 2C: 14	📄Detected

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.The linked code does not create an event for the transfer.

Recommendation

Emit an event for critical parameter changes. It is recommended emitting events for the sensitive functions that are controlled by centralization roles.

Mitigation

undefined

References:

Understanding Events in Smart Contracts

Spox-18 | Stop Transactions by using Enable Trade.

Category	Severity	Location	Status
Logical Issue	🔴 Critical	Sporx.sol: L: 263 C: 14	Detected

Description

Enable Trade is present on the following contract and when combined with Exclude from fees it can be considered a whitelist process, this will allow anyone to trade before others and can represent and issue for the holders.

Recommendation

We recommend the project owner to carefully review this function and avoid problems when performing both actions.

Mitigation

undefined

References:

Writing Clean Code for Solidity: Best Practices for Solidity Development

Technical Findings Summary
Classification of Risk

Severity	Description
🔴 Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
🟠 High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
🟡 Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
🟢 Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
ⓘ Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
🔴 Critical	1	1	0
🟠 High	0	0	0
🟡 Medium	0	0	1
🟢 Low	2	2	0
ⓘ Informational	0	1	0
Total	3	0	0

Social Media Checks

Social Media	URL	Result
Twitter	https://t.me/paxuecosystem	Pass
Other		Fail
Website	https://spox.exchange/	Pass
Telegram	https://t.me/paxuecosystem	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Assessment Results

Score Results

Review	Score
Overall Score	98/100
Auditor Score	90/100

Review by Section	Score
Manual Scan Score	40
SWC Scan Score	37
Advance Check Score	21

The Following Score System Has been Added to this page to help understand the value of the audit, the maximun score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 80 Points, if a project does not attain 80% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- The contract needs optimization and fixes.

- The contract has an Open Trade function, however, it has a validation not to close the function.

Auditor Score =90
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

CFGNINJA has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided 'as is, and CFGNINJA is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will CFGNINJA or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by CFGNINJA are subject to dependencies and are under continuing development. You agree that your access or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.