auditace.tech

AuditAce
FROM INCEPTION TO SUCCESS

Smart Contract Audit

FOR

SPACEFI

DATED : 30 Jan, 2024

MANUAL TESTING

Centralization – Owner Can Mint Tokens

Severity: High

Function: Mint

Status: Acknowledge

Overview:

The owner can mint unlimited tokens which is not recommended as this functionality can cause the token to lose it's value and the owner can also use it to manipulate the price of the token.

```
function mint(address _to, uint256 _amount) public onlyOwner {
        _mint(_to, _amount);
        _moveDelegates(address(0), _delegates[_to], _amount);
    }
```

Suggestion:

It is recommended that the total supply of the. Tokens should not be changed after initial deployment.

Explanation from Project Team:

Defi products will have a mint function to mint tokens to pay APY to the LP provider. It’s owner is another Smart contract. We have an automatic tax burning mechanism and the number of mints issued will not be equal to the number of tokens burned.

AUDIT SUMMARY

Project name – SPACEFI

Date: 30 Jan, 2024

Scope of Audit- Audit Ace was consulted to conduct the smart contract audit of the solidity source codes.

Audit Status: **High Risk Major Flag**

Issues Found

Status	Critical	High	Medium	Low	Suggestion
Open	0	0	0	3	1
Acknowledged	0	1	0	0	0
Resolved	0	0	0	0	0

USED TOOLS

Tools:

1- Manual Review:
A line by line code review has been performed by audit ace team.

2- BSC Test Network: All tests were conducted on the BSC Test network, and each test has a corresponding transaction attached to it. These tests can be found in the "Functional Tests" section of the report.

3- Slither :
The code has undergone static analysis using Slither.

Testnet version:
The tests were performed using the contract deployed on the BSC Testnet, which can be found at the following address:
https://testnet.bscscan.com/address/0x8be091713e71cf8efbc19c52d58fabb81aab4223#code

Token Information

Token Name : SPACEFI

Token Symbol: SPF

Decimals: 18

Token Supply: 2000000000

Network: BscScan

Token Type: BEP-20

Token Address:
0xe325E3Fb6F1CE9eD41160c34627d23afCB7C0059

Checksum:
Fe1c3a4fbb6e83e8393a57617b5a5b22

Owner:
0xe573Cdbf99C230865ed3a5069de6B1B1d528e45c
(at time of writing the audit)

Deployer:
0x8fE091c76D372204715D1819747cb4b41baDD49C

TOKEN OVERVIEW

Fees:

Buy Fee: 3-5%

Sell Fee: 3-5%

Transfer Fee: 0%

Fees Privilege: Owner

Ownership: Owned by another Smart contract

Minting: Yes

Max Tx Amount/ Max Wallet Amount: No

Blacklist: No

AUDIT METHODOLOGY

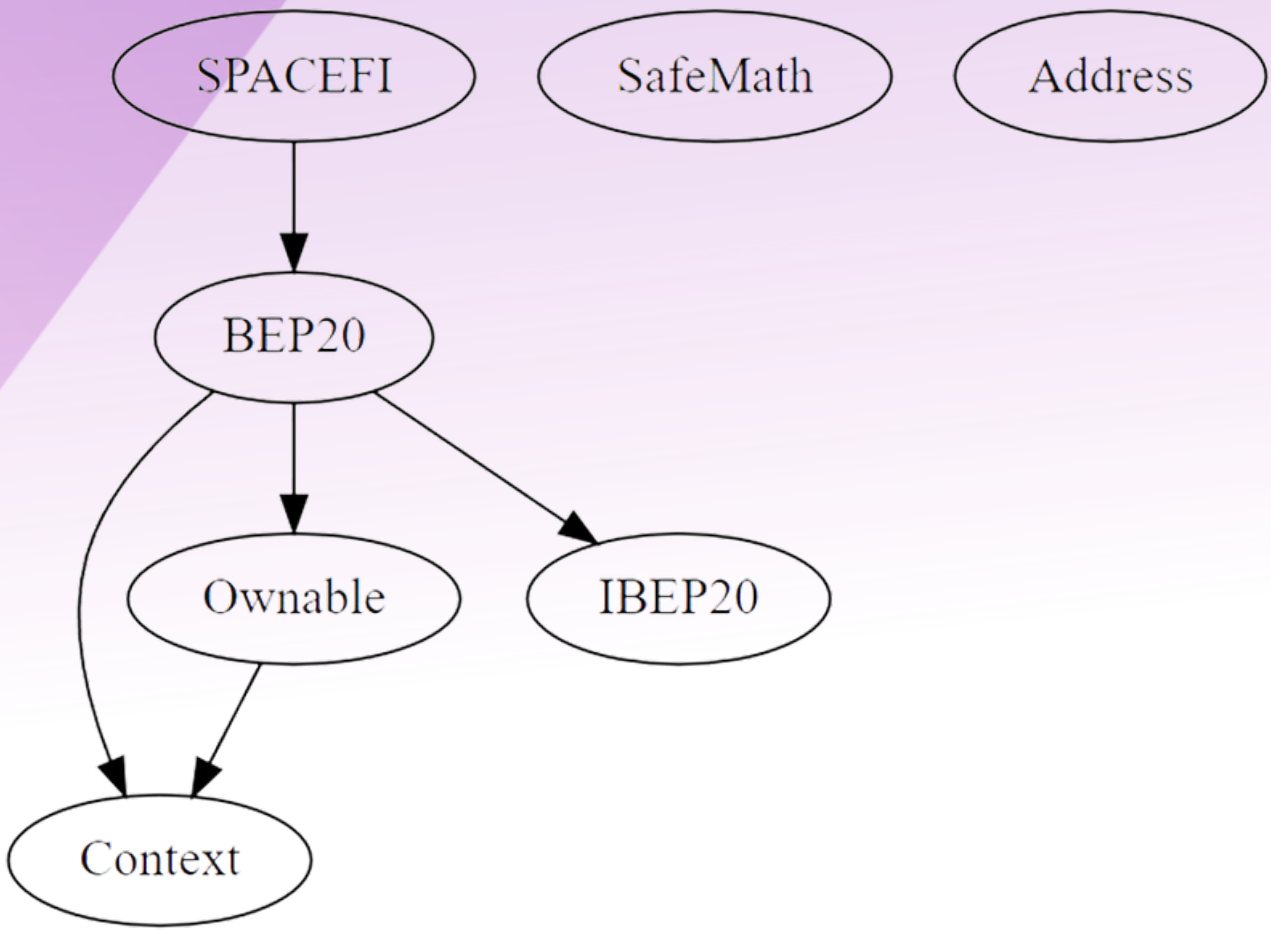
The auditing process will follow a routine as special considerations by Auditace:

- Review of the specifications, sources, and instructions provided to Auditace to make sure the contract logic meets the intentions of the client without exposing the user's funds to risk.
- Manual review of the entire codebase by our experts, which is the process of reading source code line-by-line in an attempt to identify potential vulnerabilities.
- Specification comparison is the process of checking whether the code does what the specifications, sources, and instructions provided to Auditace describe.
- Test coverage analysis determines whether the test cases are covering the code and how much code isexercised when we run the test cases.
- Symbolic execution is analysing a program to determine what inputs cause each part of a program to execute.
- Reviewing the codebase to improve maintainability, security, and control based on the established industry and academic practices.

VULNERABILITY CHECKLIST

- Return values of low-level calls
- Private modifier
- Multiple Sends
- Using Suicide
- Gas Limitand Loops
- Address hardcoded
- Exception Disorder
- Using inline assembly
- Divide before multiply
- Missing Zero Address Validation
- Compiler version not fixed
- **Gasless Send**
- Using block.timestamp
- Re-entrancy
- Tautology or contradiction
- Timestamp Dependence
- Revert/require functions
- Use of tx.origin
- Integer overflow/underflow
- Dangerous strict equalities
- Using SHA3
- Using throw

INHERITANCE TREE



STATIC ANALYSIS

A static analysis of the code was performed using Slither.

No issues were found.

```
INFO:Detectors:
SPACEFI._writeCheckpoint(address,uint32,uint256,uint256) (SPACEFI.sol#564-582) uses a dangerous strict equality:
        - nCheckpoints > 0 && checkpoints[delegatee][nCheckpoints - 1].fromBlock == blockNumber (SPACEFI.sol#574)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dangerous-strict-equalities
INFO:Detectors:
BEP20.constructor(string,string).name (SPACEFI.sol#216) shadows:
        - BEP20.name() (SPACEFI.sol#226-228) (function)
        - IBEP20.name() (SPACEFI.sol#66) (function)
BEP20.constructor(string,string).symbol (SPACEFI.sol#216) shadows:
        - BEP20.symbol() (SPACEFI.sol#230-232) (function)
        - IBEP20.symbol() (SPACEFI.sol#64) (function)
BEP20.allowance(address,address).owner (SPACEFI.sol#251) shadows:
        - Ownable.owner() (SPACEFI.sol#35-37) (function)
BEP20._approve(address,address,uint256).owner (SPACEFI.sol#308) shadows:
        - Ownable.owner() (SPACEFI.sol#35-37) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
SPACEFI.setMarketingPool(address)._marketingPool (SPACEFI.sol#361) lacks a zero-check on :
                - marketingPool = _marketingPool (SPACEFI.sol#362)
SPACEFI.setDev(address)._dev (SPACEFI.sol#366) lacks a zero-check on :
                - dev = _dev (SPACEFI.sol#367)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
SPACEFI.delegateBySig(address,uint256,uint256,uint8,bytes32,bytes32) (SPACEFI.sol#448-489) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(now <= expiry,SPACEFI::delegateBySig: signature expired) (SPACEFI.sol#487)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.isContract(address) (SPACEFI.sol#136-143) uses assembly
        - INLINE ASM (SPACEFI.sol#139-141)
Address._functionCallWithValue(address,bytes,uint256,string) (SPACEFI.sol#181-201) uses assembly
        - INLINE ASM (SPACEFI.sol#193-196)
SPACEFI.getChainId() (SPACEFI.sol#589-593) uses assembly
        - INLINE ASM (SPACEFI.sol#591)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Pragma version>=0.6.0<0.8.0 (SPACEFI.sol#10) is too complex
Pragma version>=0.6.0<0.8.0 (SPACEFI.sol#23) is too complex
Pragma version>=0.6.4 (SPACEFI.sol#56) allows old versions
Pragma version>=0.6.0<0.8.0 (SPACEFI.sol#85) is too complex
Pragma version>=0.4.0 (SPACEFI.sol#204) allows old versions
Pragma version0.6.12 (SPACEFI.sol#321) allows old versions
solc-0.6.12 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (SPACEFI.sol#145-149):
        - (success) = recipient.call{value: amount}() (SPACEFI.sol#147)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (SPACEFI.sol#181-201):
        - (success,returndata) = target.call{value: weiValue}(data) (SPACEFI.sol#188)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter SPACEFI.setMarketingPool(address)._marketingPool (SPACEFI.sol#361) is not in mixedCase
Parameter SPACEFI.setDev(address)._dev (SPACEFI.sol#366) is not in mixedCase
Parameter SPACEFI.updateMaxTransferAmountRate(uint16)._maxTransferAmountRate (SPACEFI.sol#371) is not in mixedCase
Parameter SPACEFI.setLiquidityPoolStatus(address,bool)._lpAddress (SPACEFI.sol#383) is not in mixedCase
Parameter SPACEFI.setLiquidityPoolStatus(address,bool)._status (SPACEFI.sol#383) is not in mixedCase
Parameter SPACEFI.setTaxes(uint8,uint8)._sellTax (SPACEFI.sol#407) is not in mixedCase
Parameter SPACEFI.setTaxes(uint8,uint8)._buyTax (SPACEFI.sol#407) is not in mixedCase
Parameter SPACEFI.mint(address,uint256)._to (SPACEFI.sol#415) is not in mixedCase
Parameter SPACEFI.mint(address,uint256)._amount (SPACEFI.sol#415) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Redundant expression "this (SPACEFI.sol#18)" inContext (SPACEFI.sol#12-21)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
SPACEFI.constructor() (SPACEFI.sol#344-351) uses literals with too many digits:
        - mint(_msgSender(),2000000000 * 1000000000000000000) (SPACEFI.sol#350)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Slither:SPACEFI.sol analyzed (7 contracts with 93 detectors), 45 result(s) found
```

Functional Tests

1- Approve (passed):
https://testnet.bscscan.com/tx/0x2c588bdb72a74b4e49966af0687377659cf069ac76b40b089d1ead7c5243e639

2- Set Marketing Pool (passed):
https://testnet.bscscan.com/tx/0x197db5bf3309bd5c481a114c5f54fdd064d49e9885901089359fba1eda43a3f2

3- Set Dev (passed):
https://testnet.bscscan.com/tx/0x77eedecda3cb122f19ddb401360710d2df0712a72db8626a5b7d39c8947d41e3

4- Mint (passed):
https://testnet.bscscan.com/tx/0xb2845dc8912911e3045e7b68b0ecfb225341331e3c414c1ded999750cb345955

5- Set Taxes (passed):
https://testnet.bscscan.com/tx/0x3bbc70714c8aace208969685132c8cd302600463b9f347c47d31ede8f83d02f5

CLASSIFICATION OF RISK

Severity	Description
Critical	These vulnerabilities could be exploited easily and can lead to asset loss, data loss, asset, or data manipulation. They should be fixed right away.
High-Risk	A vulnerability that affects the desired outcome when using a contract, or provides the opportunity to use a contract in an unintended way.
Medium-Risk	A vulnerability that could affect the desired outcome of executing the contract in a specific scenario.
Low-Risk	A vulnerability that does not have a significant impact on possible scenarios for the use of the contract and is probably subjective.
Gas Optimization /Suggestion	A vulnerability that has an informational character but is not affecting any of the code.

Findings

Severity	Found
Critical	0
High-Risk	1
Medium-Risk	0
Low-Risk	3
Gas Optimization / Suggestions	1

MANUAL TESTING

Centralization – Owner Can Mint Tokens

Severity: High

Function: Mint

Status: Acknowledge

Overview:

The owner can mint unlimited tokens which is not recommended as this functionality can cause the token to lose it's value and the owner can also use it to manipulate the price of the token.

```
function mint(address _to, uint256 _amount) public onlyOwner {
        _mint(_to, _amount);
        _moveDelegates(address(0), _delegates[_to], _amount);
    }
```

Suggestion:

It is recommended that the total supply of the. Tokens should not be changed after initial deployment.

Explanation from Project Team:

Defi products will have a mint function to mint tokens to pay APY to the LP provider. It’s owner is another Smart contract. We have an automatic tax burning mechanism and the number of mints issued will not be equal to the number of tokens burned.

MANUAL TESTING

Centralization – Local Variable Shadowing

Severity: Low

Status: Open

Function: _approve and allowance

Overview:

```
function allowance(address owner, address spender) public override view returns
(uint256) {
        return _allowances[owner][spender];
    }
function _approve (address owner, address spender, uint256 amount) internal {
        require(owner != address(0), 'BEP20: approve from the zero address');
        require(spender != address(0), 'BEP20: approve to the zero address');
        _allowances[owner][spender] = amount;
        emit Approval(owner, spender, amount);
    }
```

Suggestion:

Rename the local variable that shadows another component.

MANUAL TESTING

Centralization – Missing Zero Address

Severity: Low

Status: Open

Function: setMarketingPool

Overview:

Functions can take a zero address as a parameter (0x00000...). If a function parameter of address type is not properly validated by checking for zero addresses, there could be serious consequences for the contract's functionality.

```
function setMarketingPool(address _marketingPool) public onlyOperator {
        marketingPool = _marketingPool;
        emit ChangeMarketingPool(_marketingPool);
    }
```

Suggestion:

It is suggested that the address should not be zero or dead.

MANUAL TESTING

Optimization

Severity: Low

Function: Old Pragma Solidity version

Status: Open

Overview:

It is considered best practice to pick one compiler version and stick with it. With a floating pragma, contracts may accidentally be deployed using an outdated.

```
pragma solidity 0.6.12;
```

Suggestion:

Adding the latest constant version of solidity is recommended, as this prevents the unintentional deployment of a contract with an outdated compiler that contains unresolved bugs.

MANUAL TESTING

Optimization

Severity: Informational

Function: Remove unused code.

Status: Open

Overview:

Unused variables are allowed in Solidity, and they do. not pose a direct security issue. It is the best practice. though to avoid them.

```
function _msgData() internal view virtual returns (bytes calldata) {
        return msg.data;
    }
function sendValue(address payable recipient, uint256 amount) internal {
        require(address(this).balance >= amount, 'Address: insufficient balance');
        (bool success, ) = recipient.call{value: amount}('');
        require(success, 'Address: unable to send value, recipient may have revert-
ed');
    }
```

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed. The Auditace team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Auditace receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token. The Auditace team disclaims any liability for the resulting losses.

ABOUT AUDITACE

We specializes in providing thorough and reliable audits for Web3 projects. With a team of experienced professionals, we use cutting-edge technology and rigorous methodologies to evaluate the security and integrity of blockchain systems. We are committed to helping our clients ensure the safety and transparency of their digital assets and transactions.

https://auditace.tech/

https://t.me/Audit_Ace

https://twitter.com/auditace_

https://github.com/Audit-Ace