Pi Classic

Smart Contract Audit Report

SYSFIXED

05 Jan 2023

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Pi Classic	PIC	Binance Smart Chain

Addresses

Contract address	0x4Ca06992C5056e474885efB71304a9aF240D6e71
Contract deployer address	0x2B337e5695a51a6334874cEf725a47430E694021

Project Website

https://piclassic.com/

Codebase

https://bscscan.com/address/0x4Ca06992C5056e474885efB71304a9aF240D6e71#code

SUMMARY

Earn πc just by holding. Ownership renounce right before launch 50% burned, 3141 years lp lock, low 3.14% tax, presale goal: 3.14 bnb, launch goal: at least 314x, huge marketing at launch, cmc & cg fast track, welcome to the revolution.

Contract Summary

Documentation Quality

Pi Classic provides a very good documentation with standard of solidity base code.

- The technical description is provided clearly and structured and also dont have any high risk issue.

Code Quality

The Overall quality of the basecode is standard.

- Standard solidity basecode and rules are already followed by Pi Classic with the discovery of several low issues.

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 48, 49, 50, 51, 52, 54, 131, 192, 194, 197, 198, 198, 208, 223, 287, 514, 516, 634, 950 and 516.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 17.
- 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 311, 515, 516, 516, 635, 635, 636, 637, 801, 802, 1001 and 1002.

CONCLUSION

We have audited the NamaFile project released on January 2023 to discover issues and identify potential security vulnerabilities in NamaFile Project. This process is used to find technical issues and security loopholes which might be found in the smart contract.

The security audit report provides a satisfactory result with some low-risk issues.

The issues found in the NamaFile smart contract code do not pose a considerable risk. The writing of the contract is close to the standard of writing contracts in general. The low-risk issues found are some arithmetic operation issues, floating pragma is set, and out of bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value.

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

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

SMART CONTRACT ANALYSIS

Started	Wednesday Jan 04 2023 16:02:59 GMT+0000 (Coordinated Universal Time)
Finished	Thursday Jan 05 2023 15:31:15 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	PiClassicToken.sol

Detected Issues

ID	Title	Severity	Status
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "+" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "**" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "*" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "%" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "/" DISCOVERED	low	acknowledged

SWC-101	ARITHMETIC OPERATION "+=" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "-" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	ARITHMETIC OPERATION "++" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 48

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
47   library SafeMath {
48   function add(uint256 a, uint256 b) internal pure returns (uint256) {return a + b;}
49   function sub(uint256 a, uint256 b) internal pure returns (uint256) {return a - b;}
50   function mul(uint256 a, uint256 b) internal pure returns (uint256) {return a * b;}
51   function div(uint256 a, uint256 b) internal pure returns (uint256) {return a / b;}
52
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 49

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
48   function add(uint256 a, uint256 b) internal pure returns (uint256) {return a + b;}
49   function sub(uint256 a, uint256 b) internal pure returns (uint256) {return a - b;}
50   function mul(uint256 a, uint256 b) internal pure returns (uint256) {return a * b;}
51   function div(uint256 a, uint256 b) internal pure returns (uint256) {return a / b;}
52   function mod(uint256 a, uint256 b) internal pure returns (uint256) {return a % b;}
53
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 50

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
49   function sub(uint256 a, uint256 b) internal pure returns (uint256) {return a - b;}
50   function mul(uint256 a, uint256 b) internal pure returns (uint256) {return a * b;}
51   function div(uint256 a, uint256 b) internal pure returns (uint256) {return a / b;}
52   function mod(uint256 a, uint256 b) internal pure returns (uint256) {return a % b;}
53   function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
54
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 51

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
50   function mul(uint256 a, uint256 b) internal pure returns (uint256) {return a * b;}
51   function div(uint256 a, uint256 b) internal pure returns (uint256) {return a / b;}
52   function mod(uint256 a, uint256 b) internal pure returns (uint256) {return a % b;}
53   function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
54   unchecked { require(b <= a, errorMessage); return a - b; }
55
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 52

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
51   function div(uint256 a, uint256 b) internal pure returns (uint256) {return a / b;}
52   function mod(uint256 a, uint256 b) internal pure returns (uint256) {return a % b;}
53   function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
54   unchecked { require(b <= a, errorMessage); return a - b; }
55   }
56
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 54

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
53   function sub(uint256 a, uint256 b, string memory errorMessage) internal pure returns
(uint256) {
54   unchecked { require(b <= a, errorMessage); return a - b; }
55   }
56   }
57   library Address {
58
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 131

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
130   _owner = address(0);
131   _lockTime = block.timestamp + time;
132   emit OwnershipTransferred(_owner, address(0));
133   }
134   function unlock() public virtual {
135
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 192

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
191
192   uint16 internal constant FEES_DIVISOR = 10**3;
193   uint8 internal constant DECIMALS = 9;
194   uint256 internal constant ZEROES = 10**DECIMALS;
195
196
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 194

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
193   uint8 internal constant DECIMALS = 9;
194   uint256 internal constant ZEROES = 10**DECIMALS;
195
196   uint256 private constant MAX = ~uint256(0);
197   uint256 internal constant TOTAL_SUPPLY = 31415 * ZEROES;
198
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 197

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
196   uint256 private constant MAX = ~uint256(0);
197   uint256 internal constant TOTAL_SUPPLY = 31415 * ZEROES;
198   uint256 internal _reflectedSupply = (MAX - (MAX % TOTAL_SUPPLY));
199
200   /**
201
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 198

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
197   uint256 internal constant TOTAL_SUPPLY = 31415 * ZEROES;
198   uint256 internal _reflectedSupply = (MAX - (MAX % TOTAL_SUPPLY));
199
200   /**
201   * @dev Set the maximum transaction amount allowed in a transfer.
202
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 198

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
197   uint256 internal constant TOTAL_SUPPLY = 31415 * ZEROES;
198   uint256 internal _reflectedSupply = (MAX - (MAX % TOTAL_SUPPLY));
199
200   /**
201   * @dev Set the maximum transaction amount allowed in a transfer.
202
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 208

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
207   */
208   uint256 internal constant maxTransactionAmount = TOTAL_SUPPLY / 100; // 1% of the
total supply
209
210   /**
211   * @dev Set the number of tokens to swap and add to liquidity.
212
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 223

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
222   */
223   uint256 internal constant numberOfTokensToSwapToLiquidity = TOTAL_SUPPLY / 1000; //
0.1% of the total supply
224
225   // --------------------- Fees Settings ------------------- //
226
227
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 287

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
286   fees.push( Fee(name, value, recipient, 0 ) );
287   sumOfFees += value;
288   }
289
290   function _addFees() private {
291
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 514

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
513   require(_isExcludedFromRewards[account], "Account is not excluded");
514   for (uint256 i = 0; i < _excluded.length; i++) {
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 516

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518   _isExcludedFromRewards[account] = false;
519   _excluded.pop();
520
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 634

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
633   */
634   for (uint256 i = 0; i < _excluded.length; i++) {
635   if (_reflectedBalances[_excluded[i]] > rSupply || _balances[_excluded[i]] >
tSupply) return (_reflectedSupply, TOTAL_SUPPLY);
636   rSupply = rSupply.sub(_reflectedBalances[_excluded[i]]);
637   tSupply = tSupply.sub(_balances[_excluded[i]]);
638
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 950

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
949   uint256 feesCount = _getFeesCount();
950   for (uint256 index = 0; index < feesCount; index++ ){
951   (FeeType name, uint256 value, address recipient,) = _getFee(index);
952   // no need to check value < 0 as the value is uint (i.e. from 0 to 2^256-1)
953   if ( value == 0 ) continue;
954
```

SWC-101 | COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED

LINE 516

low SEVERITY

This plugin produces issues to support false positive discovery within mythril.

Source File

- PiClassicToken.sol

Locations

```
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518   _isExcludedFromRewards[account] = false;
519   _excluded.pop();
520
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 17

low SEVERITY

The current pragma Solidity directive is ""^0.8.4"". 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

- PiClassicToken.sol

Locations

```
16
17   pragma solidity ^0.8.4;
18
19   /**
20   * Tokenomics:
21
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 311

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
310   require( index >= 0 && index < fees.length, "FeesSettings._getFeeStruct: Fee index
out of bounds");
311   return fees[index];
312   }
313   function _getFee(uint256 index) internal view returns (FeeType, uint256, address,
uint256){
314   Fee memory fee = _getFeeStruct(index);
315
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 515

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
514   for (uint256 i = 0; i < _excluded.length; i++) {
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518   _isExcludedFromRewards[account] = false;
519
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 516

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518   _isExcludedFromRewards[account] = false;
519   _excluded.pop();
520
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 516

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
515   if (_excluded[i] == account) {
516   _excluded[i] = _excluded[_excluded.length - 1];
517   _balances[account] = 0;
518   _isExcludedFromRewards[account] = false;
519   _excluded.pop();
520
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 635

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
634   for (uint256 i = 0; i < _excluded.length; i++) {
635   if (_reflectedBalances[_excluded[i]] > rSupply || _balances[_excluded[i]] >
tSupply) return (_reflectedSupply, TOTAL_SUPPLY);
636   rSupply = rSupply.sub(_reflectedBalances[_excluded[i]]);
637   tSupply = tSupply.sub(_balances[_excluded[i]]);
638   }
639
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 635

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
634   for (uint256 i = 0; i < _excluded.length; i++) {
635   if (_reflectedBalances[_excluded[i]] > rSupply || _balances[_excluded[i]] >
tSupply) return (_reflectedSupply, TOTAL_SUPPLY);
636   rSupply = rSupply.sub(_reflectedBalances[_excluded[i]]);
637   tSupply = tSupply.sub(_balances[_excluded[i]]);
638   }
639
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 636

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
635   if (_reflectedBalances[_excluded[i]] > rSupply || _balances[_excluded[i]] >
tSupply) return (_reflectedSupply, TOTAL_SUPPLY);
636   rSupply = rSupply.sub(_reflectedBalances[_excluded[i]]);
637   tSupply = tSupply.sub(_balances[_excluded[i]]);
638   }
639   if (tSupply == 0 || rSupply < _reflectedSupply.div(TOTAL_SUPPLY)) return
(_reflectedSupply, TOTAL_SUPPLY);
640
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 637

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
636   rSupply = rSupply.sub(_reflectedBalances[_excluded[i]]);
637   tSupply = tSupply.sub(_balances[_excluded[i]]);
638   }
639   if (tSupply == 0 || rSupply < _reflectedSupply.div(TOTAL_SUPPLY)) return
(_reflectedSupply, TOTAL_SUPPLY);
640   return (rSupply, tSupply);
641
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 801

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
800   address[] memory path = new address[](2);
801   path[0] = address(this);
802   path[1] = _router.WETH();
803
804   _approveDelegate(address(this), address(_router), tokenAmount);
805
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 802

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
801   path[0] = address(this);
802   path[1] = _router.WETH();
803
804   _approveDelegate(address(this), address(_router), tokenAmount);
805
806
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1001

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
1000   address [] memory path = new address[](2);
1001   path[0] = address(this);
1002   path[1] = _router.WETH();
1003
1004   uint256 tAmount = amount.mul(fee).div(FEES_DIVISOR);
1005
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1002

low SEVERITY

The index access expression can cause an exception in case of use of invalid array index value.

Source File

- PiClassicToken.sol

Locations

```
1001   path[0] = address(this);
1002   path[1] = _router.WETH();
1003
1004   uint256 tAmount = amount.mul(fee).div(FEES_DIVISOR);
1005   uint256 rAmount = tAmount.mul(currentRate);
1006
```

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.