RYOSHI TOKEN

Smart Contract Audit Report

SYSFIXED

09 Jul 2021

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
RYOSHI TOKEN	RYOSHI	Binance Smart Chain

Addresses

Contract address	0x0e5f989ce525acc4ee45506af91964f7f4c9f2e9
Contract deployer address	0xa03EE3EcF4Ee6B2fc757FEC41110900d9650aCef

Project Website

https://ryoshitoken.com/

Codebase

https://bscscan.com/address/0x0e5f989ce525acc4ee45506af91964f7f4c9f2e9#code

SUMMARY

Decentralized Currency from People to People If 2021 taught the crypto world anything, it's that community-driven meme tokens are in high demand. The people want control of their token, and strong communities of HODLers can be built that have each other's back Ryoshi Success Goals That's why Ryoshi has stepped out of the shadows. See, Ryoshi is Shiba's older, wiser father. He's proud of everything his son has accomplished, but is pretty bummed about the fact that so many people missed their chance to get on the moon rocket. Ryoshi has created a decentralized, deflationary, community token that is by the people, for the people. Ryoshi solves the significant issues of Doge and Shiba — while maintaining the same meme community energy that allowed both assets to rise dramatically. Low Fees One of the major drawbacks of Shiba, and likely the reason the token has stalled out since its initial rise, is the high transaction fees associated with the Ethereum Blockchain upon which it is built. Being a BEP20 token built on the Binance Smart Chain allows Ryoshi to have tiny transaction fees. Transparency An engaged, voracious community deserves full transparency from the asset they love. That's why Ryoshi is now, and will continue to be the most transparent meme token on the market.

Contract Summary

Documentation Quality

RYOSHI TOKEN 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 RYOSHI TOKEN 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 120, 152, 175, 176, 211, 247, 485, 486, 487, 487, 488, 489, 490, 606, 608, 624, 625, 626, 789 and 608.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 7.

- 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 607, 608, 608, 790, 790, 791 and 792.

CONCLUSION

We have audited the RYOSHI TOKEN project released on July 2021 to discover issues and identify potential security vulnerabilities in RYOSHI TOKEN 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 satisfactory results with low-risk issues.

The issues found in the RYOSHI TOKEN 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, a floating pragma is set, and out-of-bounds array access which the index access expression can cause an exception in case an invalid array index value is used. The current pragma Solidity directive is ""^0.8.2"". 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.

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	Thursday Jul 08 2021 03:51:41 GMT+0000 (Coordinated Universal Time)
Finished	Friday Jul 09 2021 01:21:55 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	CoinToken.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-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 120

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
119   function add(uint256 a, uint256 b) internal pure returns (uint256) {
120   uint256 c = a + b;
121   require(c >= a, "SafeMath: addition overflow");
122
123   return c;
124
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 152

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
151   require(b <= a, errorMessage);
152   uint256 c = a - b;
153
154   return c;
155   }
156
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 175

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
174
175   uint256 c = a * b;
176   require(c / a == b, "SafeMath: multiplication overflow");
177
178   return c;
179
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 176

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
175   uint256 c = a * b;
176   require(c / a == b, "SafeMath: multiplication overflow");
177
178   return c;
179   }
180
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 211

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
210   require(b > 0, errorMessage);
211   uint256 c = a / b;
212   // assert(a == b * c + a % b); // There is no case in which this doesn't hold
213
214   return c;
215
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 247

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
246   require(b != 0, errorMessage);
247   return a % b;
248   }
249   }
250
251
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 485

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
484   _DECIMALS = _decimals;
485   _DECIMALFACTOR = 10 ** _DECIMALS;
486   _tTotal =_supply * _DECIMALFACTOR;
487   _rTotal = (_MAX - (_MAX % _tTotal));
488   _TAX_FEE = _txFee* 100;
489
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 486

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
485   _DECIMALFACTOR = 10 ** _DECIMALS;
486   _tTotal =_supply * _DECIMALFACTOR;
487   _rTotal = (_MAX - (_MAX % _tTotal));
488   _TAX_FEE = _txFee* 100;
489   _BURN_FEE = _burnFee * 100;
490
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 487

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
486   _tTotal =_supply * _DECIMALFACTOR;
487   _rTotal = (_MAX - (_MAX % _tTotal));
488   _TAX_FEE = _txFee* 100;
489   _BURN_FEE = _burnFee * 100;
490   _CHARITY_FEE = _charityFee* 100;
491
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 487

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
486   _tTotal =_supply * _DECIMALFACTOR;
487   _rTotal = (_MAX - (_MAX % _tTotal));
488   _TAX_FEE = _txFee* 100;
489   _BURN_FEE = _burnFee * 100;
490   _CHARITY_FEE = _charityFee* 100;
491
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 488

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
487   _rTotal = (_MAX - (_MAX % _tTotal));
488   _TAX_FEE = _txFee* 100;
489   _BURN_FEE = _burnFee * 100;
490   _CHARITY_FEE = _charityFee* 100;
491   ORIG_TAX_FEE = _TAX_FEE;
492
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 489

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
488   _TAX_FEE = _txFee* 100;
489   _BURN_FEE = _burnFee * 100;
490   _CHARITY_FEE = _charityFee* 100;
491   ORIG_TAX_FEE = _TAX_FEE;
492   ORIG_BURN_FEE = _BURN_FEE;
493
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 490

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
489   _BURN_FEE = _burnFee * 100;
490   _CHARITY_FEE = _charityFee* 100;
491   ORIG_TAX_FEE = _TAX_FEE;
492   ORIG_BURN_FEE = _BURN_FEE;
493   ORIG_CHARITY_FEE = _CHARITY_FEE;
494
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 606

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
605   require(_isExcluded[account], "Account is already included");
606   for (uint256 i = 0; i < _excluded.length; i++) {
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 608

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610   _isExcluded[account] = false;
611   _excluded.pop();
612
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 624

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
623   require(_txFee < 100 && _burnFee < 100 && _charityFee < 100);
624   _TAX_FEE = _txFee* 100;
625   _BURN_FEE = _burnFee * 100;
626   _CHARITY_FEE = _charityFee* 100;
627   ORIG_TAX_FEE = _TAX_FEE;
628
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 625

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
624   _TAX_FEE = _txFee* 100;
625   _BURN_FEE = _burnFee * 100;
626   _CHARITY_FEE = _charityFee* 100;
627   ORIG_TAX_FEE = _TAX_FEE;
628   ORIG_BURN_FEE = _BURN_FEE;
629
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 626

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
625   _BURN_FEE = _burnFee * 100;
626   _CHARITY_FEE = _charityFee* 100;
627   ORIG_TAX_FEE = _TAX_FEE;
628   ORIG_BURN_FEE = _BURN_FEE;
629   ORIG_CHARITY_FEE = _CHARITY_FEE;
630
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 789

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
788   uint256 tSupply = _tTotal;
789   for (uint256 i = 0; i < _excluded.length; i++) {
790   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
791   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
792   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
793
```

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

LINE 608

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610   _isExcluded[account] = false;
611   _excluded.pop();
612
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 7

low SEVERITY

The current pragma Solidity directive is ""^0.8.2"". 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

- CoinToken.sol

Locations

```
6
7   pragma solidity ^0.8.2;
8
9
10   abstract contract Context {
11
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 607

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
606   for (uint256 i = 0; i < _excluded.length; i++) {
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610   _isExcluded[account] = false;
611
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 608

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610   _isExcluded[account] = false;
611   _excluded.pop();
612
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 608

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
607   if (_excluded[i] == account) {
608   _excluded[i] = _excluded[_excluded.length - 1];
609   _tOwned[account] = 0;
610   _isExcluded[account] = false;
611   _excluded.pop();
612
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 790

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
789   for (uint256 i = 0; i < _excluded.length; i++) {
790   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
791   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
792   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
793   }
794
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 790

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
789   for (uint256 i = 0; i < _excluded.length; i++) {
790   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
791   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
792   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
793   }
794
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 791

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
790   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
791   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
792   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
793   }
794   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
795
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 792

low SEVERITY

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

Source File

- CoinToken.sol

Locations

```
791   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
792   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
793   }
794   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
795   return (rSupply, tSupply);
796
```

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.