MetaPionner Token

Smart Contract Audit Report

SYSFIXED

22 Nov 2022

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
MetaPionner Token	MPI	Binance Smart Chain

Addresses

Contract address	0x82555cc48a532fa4e2194ab883eb6d465149f80e
Contract deployer address	0x24A193da3efE2404fA2C1c7b0D89Dd90f16443B4

Project Website

https://metapi.xyz/

Codebase

https://bscscan.com/address/0x82555cc48a532fa4e2194ab883eb6d465149f80e#code

SUMMARY

MetaPioneers is an NFTfi project in the Web3 space that combines the power of DeFi & NFTs to create an entertaining DApp earning its users' sustainable yield in perpetuity.

Contract Summary

Documentation Quality

MetaPionner 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 MetaPionner Token with the discovery of several low issues.

Test Coverage

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

Audit Findings Summary

- SWC-100 SWC-108 | Explicitly define visibility for all state variables on lines 1075, 1077 and 1079.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 311, 334, 367, 369, 390, 391, 416, 418, 467, 655, 656, 660, 661, 661, 662, 677, 687, 687, 690, 690, 690, 1131 and 1138.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 6.
- 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 661, 688, 689, 691, 691, 1132 and 1139.

CONCLUSION

We have audited the MetaPionner Token project released on November 2022 to discover issues and identify potential security vulnerabilities in MetaPionner 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 a satisfactory result with some low-risk issues.

The issues found in the MetaPionner 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, a state variable visibility is not 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.	ISSUE FOUND
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	Monday Nov 21 2022 20:01:38 GMT+0000 (Coordinated Universal Time)
Finished	Tuesday Nov 22 2022 01:32:17 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	MetaPionnerToken.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	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-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT 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 311

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
310   address owner = _msgSender();
311   _approve(owner, spender, allowance(owner, spender) + addedValue);
312   return true;
313   }
314
315
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 334

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
333   unchecked {
334   _approve(owner, spender, currentAllowance - subtractedValue);
335   }
336
337   return true;
338
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 367

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
366   unchecked {
367   _balances[from] = fromBalance - amount;
368   }
369   _balances[to] += amount;
370
371
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 369

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
368   }
369   _balances[to] += amount;
370
371   emit Transfer(from, to, amount);
372
373
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 390

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
389
390   _totalSupply += amount;
391   _balances[account] += amount;
392   emit Transfer(address(0), account, amount);
393
394
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 391

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
390   _totalSupply += amount;
391   _balances[account] += amount;
392   emit Transfer(address(0), account, amount);
393
394   _afterTokenTransfer(address(0), account, amount);
395
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 416

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
415   unchecked {
416   _balances[account] = accountBalance - amount;
417   }
418   _totalSupply -= amount;
419
420
```

SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 418

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
417   }
418   _totalSupply -= amount;
419
420   emit Transfer(account, address(0), amount);
421
422
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 467

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
466   unchecked {
467   _approve(owner, spender, currentAllowance - amount);
468   }
469   }
470   }
471
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 655

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
654   while (temp != 0) {
655   digits++;
656   temp /= 10;
657   }
658   bytes memory buffer = new bytes(digits);
659
```

SWC-101 | ARITHMETIC OPERATION "/=" DISCOVERED

LINE 656

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
655   digits++;
656   temp /= 10;
657   }
658   bytes memory buffer = new bytes(digits);
659   while (value != 0) {
660
```

SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 660

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
659   while (value != 0) {
660   digits -= 1;
661   buffer[digits] = bytes1(uint8(48 + uint256(value % 10)));
662   value /= 10;
663   }
664
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 661

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
660   digits -= 1;
661   buffer[digits] = bytes1(uint8(48 + uint256(value % 10)));
662   value /= 10;
663   }
664   return string(buffer);
665
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 661

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
660   digits -= 1;
661   buffer[digits] = bytes1(uint8(48 + uint256(value % 10)));
662   value /= 10;
663   }
664   return string(buffer);
665
```

SWC-101 | ARITHMETIC OPERATION "/=" DISCOVERED

LINE 662

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
661   buffer[digits] = bytes1(uint8(48 + uint256(value % 10)));
662   value /= 10;
663   }
664   return string(buffer);
665   }
666
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 677

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
676   while (temp != 0) {
677   length++;
678   temp >>= 8;
679   }
680   return toHexString(value, length);
681
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 687

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
686   function toHexString(uint256 value, uint256 length) internal pure returns (string
memory) {
687   bytes memory buffer = new bytes(2 * length + 2);
688   buffer[0] = "0";
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 687

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
686   function toHexString(uint256 value, uint256 length) internal pure returns (string
memory) {
687   bytes memory buffer = new bytes(2 * length + 2);
688   buffer[0] = "0";
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 690

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693   }
694
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 690

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693   }
694
```

SWC-101 | ARITHMETIC OPERATION "--" DISCOVERED

LINE 690

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693   }
694
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1131

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
1130   function setbuyList(address[] memory _buyList) public onlyRole(SUPER) {
1131   for(uint i=0;i<_buyList.length;i++) {
1132   buyList[_buyList[i]] = true;
1133   }
1134   }
1135
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1138

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
1137   function setsellList(address[] memory _sellList) public onlyRole(SUPER) {
1138   for(uint i=0;i<_sellList.length;i++) {
1139   sellList[_sellList[i]] = true;
1140   }
1141   }
1142
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 6

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

- MetaPionnerToken.sol

Locations

```
5   // SPDX-License-Identifier: MIT
6   pragma solidity ^0.8.4;
7
8   // OpenZeppelin Contracts (last updated v4.5.0)
(token/ERC20/extensions/ERC20Burnable.sol)
9
10
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 1075

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "realBurn" is internal. Other possible visibility settings are public and private.

Source File

- MetaPionnerToken.sol

Locations

```
1074
1075   bool realBurn;
1076   mapping(address => bool) private  buyList;
1077   bool openbuyList;
1078   mapping(address => bool) private  sellList;
1079
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 1077

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "openbuyList" is internal. Other possible visibility settings are public and private.

Source File

- MetaPionnerToken.sol

Locations

```
1076   mapping(address => bool) private  buyList;
1077   bool openbuyList;
1078   mapping(address => bool) private  sellList;
1079   bool opensellList;
1080
1081
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 1079

low SEVERITY

It is best practice to set the visibility of state variables explicitly. The default visibility for "opensellList" is internal. Other possible visibility settings are public and private.

Source File

- MetaPionnerToken.sol

Locations

```
1078   mapping(address => bool) private  sellList;
1079   bool opensellList;
1080
1081   bytes32 public constant EXTERN = bytes32(keccak256(abi.encodePacked("EXTERN")));
1082   bytes32 public constant SUPER = bytes32(keccak256(abi.encodePacked("MPI_SUPER")));
1083
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 661

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
660   digits -= 1;
661   buffer[digits] = bytes1(uint8(48 + uint256(value % 10)));
662   value /= 10;
663   }
664   return string(buffer);
665
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 688

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
687   bytes memory buffer = new bytes(2 * length + 2);
688   buffer[0] = "0";
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 689

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
688   buffer[0] = "0";
689   buffer[1] = "x";
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 691

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693   }
694   require(value == 0, "Strings: hex length insufficient");
695
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 691

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
690   for (uint256 i = 2 * length + 1; i > 1; --i) {
691   buffer[i] = _HEX_SYMBOLS[value & 0xf];
692   value >>= 4;
693   }
694   require(value == 0, "Strings: hex length insufficient");
695
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1132

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
1131   for(uint i=0;i<_buyList.length;i++) {
1132   buyList[_buyList[i]] = true;
1133   }
1134   }
1135
1136
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1139

low SEVERITY

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

Source File

- MetaPionnerToken.sol

Locations

```
1138   for(uint i=0;i<_sellList.length;i++) {
1139   sellList[_sellList[i]] = true;
1140   }
1141   }
1142
1143
```

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.