Kodexa

Smart Contract Audit Report

SYSFIXED

19 Dec 2021

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Kodexa	Kodexa	Binance Smart Chain

Addresses

Contract address	0xb007549db2a335364dfdce86001ee3b081051f03
Contract deployer address	0xC5a80c2F0BEe434362cdf3b97a19726DC7A98424

Project Website

https://mosaicalpha.com/

Codebase

https://bscscan.com/address/0xb007549db2a335364dfdce86001ee3b081051f03#code

SUMMARY

DeFi Solutions With Science and Fantasy We have designed our decentralized financial solutions to be as comfortable to use as standard banking solutions are. With our easy-to-use platform and managed token basket features, we are eager to open the world of crypto to everyone. To contribute to the increase of financial awareness around the world, we are publishing educational content about the crypto world for every user level. We have created a whole new level of asset management for professional crypto traders.

Contract Summary

Documentation Quality

Kodexa 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 Kodexa 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 937.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 567, 586, 608, 641, 643, 664, 665, 690, 692, 797, 865, 889, 1052, 1090, 1129, 1131, 1156, 1158, 1275, 1303, 1304, 1090, 1131, 1158, 1303 and 1304.
- SWC-103 | Pragma statements can be allowed to float when a contract is intended on lines 8.
- 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 935, 936, 1201, 1202, 866, 866, 890, 1053, 1130, 1131, 1131, 1157, 1158, 1158, 1276, 1277, 1277, 1278, 1303, 1303, 1304 and 1304.

CONCLUSION

We have audited the Kodexa project released on January 2023 to discover issues and identify potential security vulnerabilities in Kodexa 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 Kodexa smart contract code issues 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 are that a floating pragma is set, state variable visibility is not set, public state variable with array type causing reachable exception by default, and out-of-bounds array access. The current pragma Solidity directive is ""^0.8.0"". Specifying a fixed compiler version is recommended 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. State variable visibility is not set, the best practice is to set the visibility of state variables explicitly. The default visibility for "rolesMap" is internal. Other possible visibility settings are public and private.

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	Saturday Dec 18 2021 03:12:25 GMT+0000 (Coordinated Universal Time)
Finished	Sunday Dec 19 2021 05:29:48 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	KodexaToken.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	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-101	COMPILER-REWRITABLE "<UINT> - 1" DISCOVERED	low	acknowledged
SWC-103	A FLOATING PRAGMA IS SET.	low	acknowledged
SWC-108	STATE VARIABLE VISIBILITY IS NOT SET.	low	acknowledged
SWC-110	PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.	low	acknowledged
SWC-110	PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.	low	acknowledged
SWC-110	PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.	low	acknowledged
SWC-110	PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.	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-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 567

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
566   unchecked {
567   _approve(sender, _msgSender(), currentAllowance - amount);
568   }
569
570   return true;
571
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 586

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
585   function increaseAllowance(address spender, uint256 addedValue) public virtual
returns (bool) {
586   _approve(_msgSender(), spender, _allowances[_msgSender()][spender] + addedValue);
587   return true;
588   }
589
590
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 608

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
607   unchecked {
608   _approve(_msgSender(), spender, currentAllowance - subtractedValue);
609   }
610
611   return true;
612
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 641

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
640   unchecked {
641   _balances[sender] = senderBalance - amount;
642   }
643   _balances[recipient] += amount;
644
645
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 643

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
642   }
643   _balances[recipient] += amount;
644
645   emit Transfer(sender, recipient, amount);
646
647
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 664

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
663
664   _totalSupply += amount;
665   _balances[account] += amount;
666   emit Transfer(address(0), account, amount);
667
668
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 665

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
664   _totalSupply += amount;
665   _balances[account] += amount;
666   emit Transfer(address(0), account, amount);
667
668   _afterTokenTransfer(address(0), account, amount);
669
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 690

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
689   unchecked {
690   _balances[account] = accountBalance - amount;
691   }
692   _totalSupply -= amount;
693
694
```

SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 692

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
691   }
692   _totalSupply -= amount;
693
694   emit Transfer(account, address(0), amount);
695
696
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 797

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
796   unchecked {
797   _approve(account, _msgSender(), currentAllowance - amount);
798   }
799   _burn(account, amount);
800   }
801
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 865

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
864   // query support of each interface in interfaceIds
865   for (uint256 i = 0; i < interfaceIds.length; i++) {
866   interfaceIdsSupported[i] = _supportsERC165Interface(account, interfaceIds[i]);
867   }
868   }
869
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 889

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
888   // query support of each interface in _interfaceIds
889   for (uint256 i = 0; i < interfaceIds.length; i++) {
890   if (!_supportsERC165Interface(account, interfaceIds[i])) {
891   return false;
892   }
893
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1052

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1051   extRegistry = _extreg;
1052   for (uint i=0; i < _ownrs.length; i++)
1053   _addOwner(_ownrs[i]);
1054   }
1055
1056
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1090

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1089   uint256 intmax;
1090   unchecked { intmax = uint256(0) - 1;}
1091   uint256 tmp = rolesMap[_address] & (intmax ^ (uint256(1) << _role));
1092
1093   if (tmp == 0) {
1094
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1129

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1128   _unsetRole(_ownr, Roles.OWNER);
1129   for (uint i=0; i < owners.length; i++){
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1131

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133   break;
1134   }
1135
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1156

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1155   _unsetRole(_mgr, Roles.MANAGER);
1156   for (uint i=0; i < managers.length; i++){
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1158

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160   break;
1161   }
1162
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 1275

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1274   if (contractWhitelist[_address]) return true;
1275   for (uint256 i = 0; i < secondaryWhitelistAddresses.length; i++) {
1276   if (secondaryWhitelistAddresses[i] != address(0)) {
1277   (bool success, bytes memory data) =
secondaryWhitelistAddresses[i].staticcall(abi.encodeWithSignature(secondaryWhitelistCallS
trings[i], _address));
1278   if (success == true && data[31] > 0) return true;
1279
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1303

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1302   require(_idx < secondaryWhitelistAddresses.length);
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 1304

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307   }
1308
```

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

LINE 1090

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1089   uint256 intmax;
1090   unchecked { intmax = uint256(0) - 1;}
1091   uint256 tmp = rolesMap[_address] & (intmax ^ (uint256(1) << _role));
1092
1093   if (tmp == 0) {
1094
```

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

LINE 1131

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133   break;
1134   }
1135
```

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

LINE 1158

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160   break;
1161   }
1162
```

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

LINE 1303

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1302   require(_idx < secondaryWhitelistAddresses.length);
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307
```

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

LINE 1304

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307   }
1308
```

SWC-103 | A FLOATING PRAGMA IS SET.

LINE 8

low SEVERITY

The current pragma Solidity directive is ""^0.8.0"". 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

- KodexaToken.sol

Locations

```
7
8   pragma solidity ^0.8.0;
9
10   /**
11   * @dev Provides information about the current execution context, including the
12
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 937

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
936   address[] public owners;
937   mapping(address => uint256) rolesMap;
938   address public extRegistry;
939
940   function hasRole(address _address, uint8 _role) external view returns (bool) {
941
```

SWC-110 | PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.

LINE 935

low SEVERITY

The public state variable "managers" in "OwnableManageableChainableRoles" contract has type "address[]" and can cause an exception in case of use of invalid array index value.

Source File

- KodexaToken.sol

Locations

```
934   contract OwnableManageableChainableRoles is IExternalOwnerManagerRegistry {
935   address[] public managers;
936   address[] public owners;
937   mapping(address => uint256) rolesMap;
938   address public extRegistry;
939
```

SWC-110 | PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.

LINE 936

low SEVERITY

The public state variable "owners" in "OwnableManageableChainableRoles" contract has type "address[]" and can cause an exception in case of use of invalid array index value.

Source File

- KodexaToken.sol

Locations

```
935   address[] public managers;
936   address[] public owners;
937   mapping(address => uint256) rolesMap;
938   address public extRegistry;
939
940
```

SWC-110 | PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.

LINE 1201

low SEVERITY

The public state variable "secondaryWhitelistAddresses" in "KodexaToken" contract has type "address[]" and can cause an exception in case of use of invalid array index value.

Source File

- KodexaToken.sol

Locations

```
1200   bool private _locked;
1201   address[] public secondaryWhitelistAddresses;
1202   string[] public secondaryWhitelistCallStrings;
1203
1204   constructor(
1205
```

SWC-110 | PUBLIC STATE VARIABLE WITH ARRAY TYPE CAUSING REACHABLE EXCEPTION BY DEFAULT.

LINE 1202

low SEVERITY

The public state variable "secondaryWhitelistCallStrings" in "KodexaToken" contract has type "string[]" and can cause an exception in case of use of invalid array index value.

Source File

- KodexaToken.sol

Locations

```
1201   address[] public secondaryWhitelistAddresses;
1202   string[] public secondaryWhitelistCallStrings;
1203
1204   constructor(
1205   string memory name,
1206
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 866

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
865   for (uint256 i = 0; i < interfaceIds.length; i++) {
866   interfaceIdsSupported[i] = _supportsERC165Interface(account, interfaceIds[i]);
867   }
868   }
869
870
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 866

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
865   for (uint256 i = 0; i < interfaceIds.length; i++) {
866   interfaceIdsSupported[i] = _supportsERC165Interface(account, interfaceIds[i]);
867   }
868   }
869
870
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 890

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
889   for (uint256 i = 0; i < interfaceIds.length; i++) {
890   if (!_supportsERC165Interface(account, interfaceIds[i])) {
891   return false;
892   }
893   }
894
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1053

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1052   for (uint i=0; i < _ownrs.length; i++)
1053   _addOwner(_ownrs[i]);
1054   }
1055
1056   event ExternalRegistryAddressChanged(address addr);
1057
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1130

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1129   for (uint i=0; i < owners.length; i++){
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133   break;
1134
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1131

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133   break;
1134   }
1135
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1131

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1130   if (owners[i] == _ownr) {
1131   owners[i] = owners[owners.length-1];
1132   owners.pop();
1133   break;
1134   }
1135
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1157

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1156   for (uint i=0; i < managers.length; i++){
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160   break;
1161
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1158

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160   break;
1161   }
1162
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1158

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1157   if (managers[i] == _mgr) {
1158   managers[i] = managers[managers.length-1];
1159   managers.pop();
1160   break;
1161   }
1162
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1276

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1275   for (uint256 i = 0; i < secondaryWhitelistAddresses.length; i++) {
1276   if (secondaryWhitelistAddresses[i] != address(0)) {
1277   (bool success, bytes memory data) =
secondaryWhitelistAddresses[i].staticcall(abi.encodeWithSignature(secondaryWhitelistCallS
trings[i], _address));
1278   if (success == true && data[31] > 0) return true;
1279   }
1280
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1277

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1276   if (secondaryWhitelistAddresses[i] != address(0)) {
1277   (bool success, bytes memory data) =
secondaryWhitelistAddresses[i].staticcall(abi.encodeWithSignature(secondaryWhitelistCallS
trings[i], _address));
1278   if (success == true && data[31] > 0) return true;
1279   }
1280   }
1281
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1277

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1276   if (secondaryWhitelistAddresses[i] != address(0)) {
1277   (bool success, bytes memory data) =
secondaryWhitelistAddresses[i].staticcall(abi.encodeWithSignature(secondaryWhitelistCallS
trings[i], _address));
1278   if (success == true && data[31] > 0) return true;
1279   }
1280   }
1281
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1278

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1277   (bool success, bytes memory data) =
secondaryWhitelistAddresses[i].staticcall(abi.encodeWithSignature(secondaryWhitelistCallS
trings[i], _address));
1278   if (success == true && data[31] > 0) return true;
1279   }
1280   }
1281   return false;
1282
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1303

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1302   require(_idx < secondaryWhitelistAddresses.length);
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1303

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1302   require(_idx < secondaryWhitelistAddresses.length);
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1304

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307   }
1308
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1304

low SEVERITY

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

Source File

- KodexaToken.sol

Locations

```
1303   secondaryWhitelistAddresses[_idx] =
secondaryWhitelistAddresses[secondaryWhitelistAddresses.length - 1];
1304   secondaryWhitelistCallStrings[_idx] =
secondaryWhitelistCallStrings[secondaryWhitelistCallStrings.length - 1];
1305   secondaryWhitelistAddresses.pop();
1306   secondaryWhitelistCallStrings.pop();
1307   }
1308
```

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.