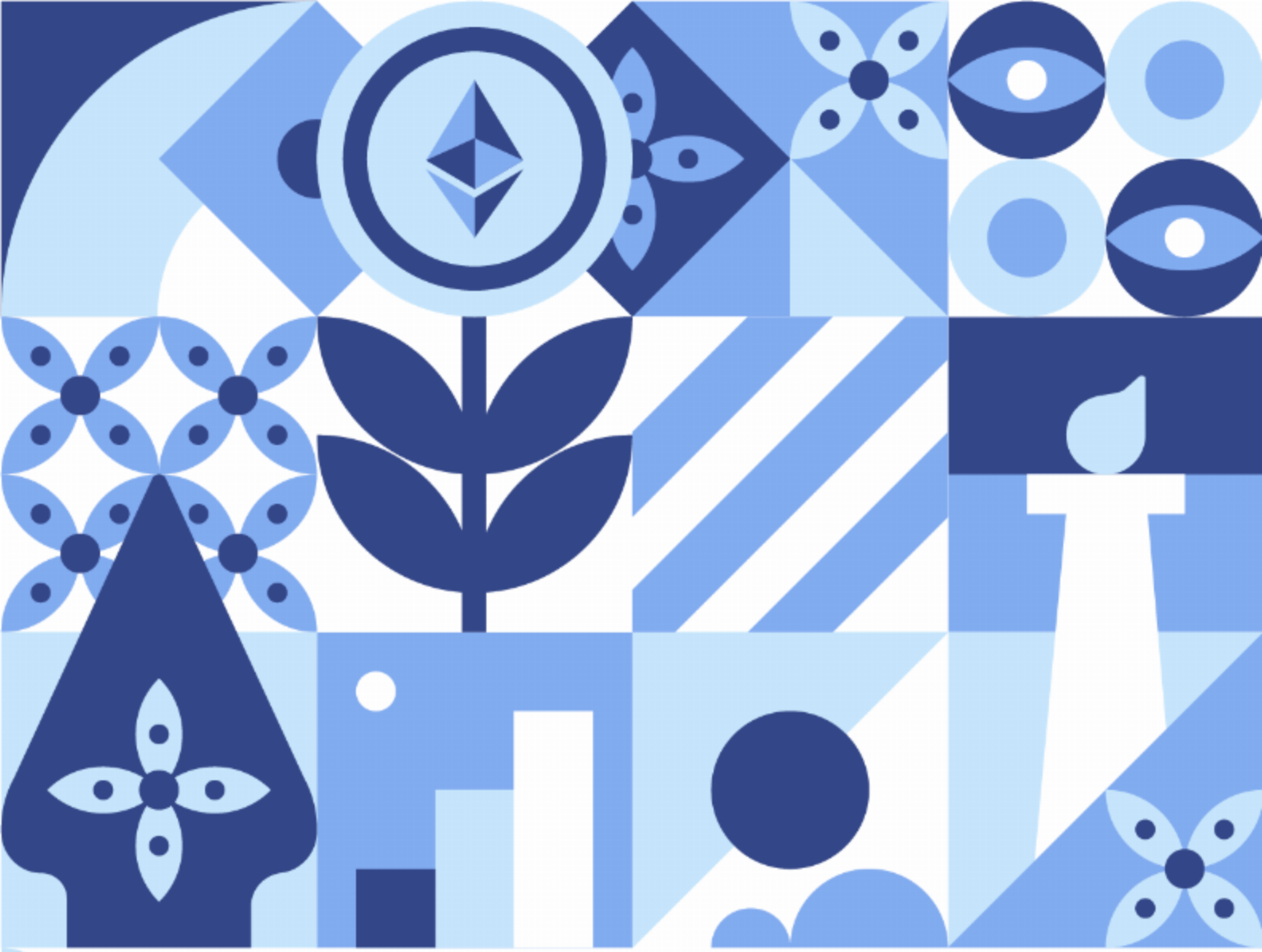

Kusunoki Samurai

Smart Contract Audit Report

SYSFIXED

16 Feb 2022

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
Kusunoki Samurai	Kusunoki	Ethereum

Addresses

Contract address	0x36919a60a2b67b6d2329863093d180d23d5a0308
Contract deployer address	0x2449265843E9aC68Ff4AB2680aeb188B6A33b1bE

Project Website

https://www.kusunokisamurai.com/

Codebase

https://etherscan.io/address/0x36919a60a2b67b6d2329863093d180d23d5a0308#code

SUMMARY

The golden age of the samurai, 14th century feudal Japan. Kusunoki Samurai is a metaverse action-adventure open world game where you, the samurai, will journey through the four realms: the Earthly Realm, the Otherworld, the Underworld and Heaven. Each realm will present a set path to explore and pursue, following the story of a unique samurai. It is here you will encounter battles, trials, and tribulations across these realms. Progression through the realms will present the opportunity for you, the player, to earn and collect valuable rewards to become the most revered samurai in the world of Kusunoki Samurai.

Contract Summary

Documentation Quality

Kusunoki Samurai 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 Kusunoki Samurai 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 724.
- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 115, 147, 170, 171, 206, 242, 458, 697, 697, 699, 699, 727, 727, 728, 728, 729, 729, 851, 853, 919, 938, 944, 993, 1165, 1165, 1169, 1169, 1183, 1183 and 853.
- 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 852, 853, 853, 920, 920, 921, 922, 1038 and 1039.

CONCLUSION

We have audited the Kusunoki Samurai project released on February 2022 to discover issues and identify potential security vulnerabilities in Kusunoki Samurai 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 Kusunoki Samurai 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 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.	PASS
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	Tuesday Feb 15 2022 10:45:39 GMT+0000 (Coordinated Universal Time)
Finished	Wednesday Feb 16 2022 21:20:11 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	KUSUNOKI.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-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-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-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged
SWC-110	OUT OF BOUNDS ARRAY ACCESS	low	acknowledged

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 115

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
114   function add(uint256 a, uint256 b) internal pure returns (uint256) {
115   uint256 c = a + b;
116   require(c >= a, "SafeMath: addition overflow");
117
118   return c;
119
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 147

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
146   require(b <= a, errorMessage);
147   uint256 c = a - b;
148
149   return c;
150   }
151
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 170

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
169
170   uint256 c = a * b;
171   require(c / a == b, "SafeMath: multiplication overflow");
172
173   return c;
174
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 171

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
170   uint256 c = a * b;
171   require(c / a == b, "SafeMath: multiplication overflow");
172
173   return c;
174   }
175
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 206

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
205   require(b > 0, errorMessage);
206   uint256 c = a / b;
207   // assert(a == b * c + a % b); // There is no case in which this doesn't hold
208
209   return c;
210
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 242

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
241   require(b != 0, errorMessage);
242   return a % b;
243   }
244   }
245
246
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 458

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
457   _owner = address(0);
458   _lockTime = block.timestamp + time;
459   emit OwnershipTransferred(_owner, address(0));
460   }
461
462
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 697

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
696   uint256 private constant MAX = ~uint256(0);
697   uint256 private _tTotal = 80000000000000000 * 10**18;
698
699   uint256 private _rTotal = (MAX - (MAX % _tTotal));
700   uint256 private _tFeeTotal;
701
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 697

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
696   uint256 private constant MAX = ~uint256(0);
697   uint256 private _tTotal = 80000000000000000 * 10**18;
698
699   uint256 private _rTotal = (MAX - (MAX % _tTotal));
700   uint256 private _tFeeTotal;
701
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 699

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
698
699   uint256 private _rTotal = (MAX - (MAX % _tTotal));
700   uint256 private _tFeeTotal;
701
702   string private _name = "Kusunoki Samurai";
703
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 699

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
698
699   uint256 private _rTotal = (MAX - (MAX % _tTotal));
700   uint256 private _tFeeTotal;
701
702   string private _name = "Kusunoki Samurai";
703
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 727

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
726
727   uint256 public numTokensSellToAddToLiquidity = 1600000000000000 * 10**18;
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 727

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
726
727   uint256 public numTokensSellToAddToLiquidity = 1600000000000000 * 10**18;
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 728

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
727   uint256 public numTokensSellToAddToLiquidity = 1600000000000000 * 10**18;
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
732
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 728

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
727   uint256 public numTokensSellToAddToLiquidity = 1600000000000000 * 10**18;
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
732
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 729

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
732   event SwapAndLiquifyEnabledUpdated(bool enabled);
733
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 729

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
728   uint256 public _maxTxAmount = 80000000000000000 * 10**18;
729   uint256 public maxWalletToken = 80000000000000000 * 10**18;
730
731   event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
732   event SwapAndLiquifyEnabledUpdated(bool enabled);
733
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 851

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
850   require(_isExcluded[account], "Account is already excluded");
851   for (uint256 i = 0; i < _excluded.length; i++) {
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 853

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855   _isExcluded[account] = false;
856   _excluded.pop();
857
```

SWC-101 | ARITHMETIC OPERATION "++" DISCOVERED

LINE 919

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
918   uint256 tSupply = _tTotal;
919   for (uint256 i = 0; i < _excluded.length; i++) {
920   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
921   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
922   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
923
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 938

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
937   return _amount.mul(_taxFee).div(
938   10**2
939   );
940   }
941
942
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 944

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
943   return _amount.mul(_liquidityFee).div(
944   10**2
945   );
946   }
947
948
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 993

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
992   uint256 contractBalanceRecepient = balanceOf(to);
993   require(contractBalanceRecepient + amount <= maxWalletToken,"Exceeds maximum wallet
token amount.");
994   }
995
996   uint256 contractTokenBalance = balanceOf(address(this));
997
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1165

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1164   function setMaxWalletTokend(uint256 _maxToken) external onlyOwner {
1165   maxWalletToken = _maxToken * (10**18);
1166   }
1167
1168   function setNumTokensSellToAddToLiquidity(uint256 newAmt) external onlyOwner() {
1169
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1165

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1164   function setMaxWalletTokend(uint256 _maxToken) external onlyOwner {
1165   maxWalletToken = _maxToken * (10**18);
1166   }
1167
1168   function setNumTokensSellToAddToLiquidity(uint256 newAmt) external onlyOwner() {
1169
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1169

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1168   function setNumTokensSellToAddToLiquidity(uint256 newAmt) external onlyOwner() {
1169   numTokensSellToAddToLiquidity = newAmt * (10**18);
1170   }
1171
1172   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
1173
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1169

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1168   function setNumTokensSellToAddToLiquidity(uint256 newAmt) external onlyOwner() {
1169   numTokensSellToAddToLiquidity = newAmt * (10**18);
1170   }
1171
1172   function setSwapAndLiquifyEnabled(bool _enabled) public onlyOwner {
1173
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 1183

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1182   require(maxTxAmount > 0, "transaction amount must be greater than zero");
1183   _maxTxAmount = maxTxAmount * (10**18);
1184   }
1185
1186   function setFees(uint256 taxFee, uint256 liquidityFee, uint256 marketingFee,
uint256 burnFee) external onlyOwner() {
1187
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 1183

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1182   require(maxTxAmount > 0, "transaction amount must be greater than zero");
1183   _maxTxAmount = maxTxAmount * (10**18);
1184   }
1185
1186   function setFees(uint256 taxFee, uint256 liquidityFee, uint256 marketingFee,
uint256 burnFee) external onlyOwner() {
1187
```

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

LINE 853

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855   _isExcluded[account] = false;
856   _excluded.pop();
857
```

SWC-108 | STATE VARIABLE VISIBILITY IS NOT SET.

LINE 724

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
723
724   bool inSwapAndLiquify;
725   bool public swapAndLiquifyEnabled = true;
726
727   uint256 public numTokensSellToAddToLiquidity = 1600000000000000 * 10**18;
728
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 852

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
851   for (uint256 i = 0; i < _excluded.length; i++) {
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855   _isExcluded[account] = false;
856
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 853

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855   _isExcluded[account] = false;
856   _excluded.pop();
857
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 853

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
852   if (_excluded[i] == account) {
853   _excluded[i] = _excluded[_excluded.length - 1];
854   _tOwned[account] = 0;
855   _isExcluded[account] = false;
856   _excluded.pop();
857
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 920

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
919   for (uint256 i = 0; i < _excluded.length; i++) {
920   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
921   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
922   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
923   }
924
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 920

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
919   for (uint256 i = 0; i < _excluded.length; i++) {
920   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
921   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
922   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
923   }
924
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 921

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
920   if (_rOwned[_excluded[i]] > rSupply || _tOwned[_excluded[i]] > tSupply) return
(_rTotal, _tTotal);
921   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
922   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
923   }
924   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
925
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 922

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
921   rSupply = rSupply.sub(_rOwned[_excluded[i]]);
922   tSupply = tSupply.sub(_tOwned[_excluded[i]]);
923   }
924   if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
925   return (rSupply, tSupply);
926
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1038

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1037   address[] memory path = new address[](2);
1038   path[0] = address(this);
1039   path[1] = uniswapV2Router.WETH();
1040
1041   _approve(address(this), address(uniswapV2Router), tokenAmount);
1042
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1039

low SEVERITY

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

Source File

- KUSUNOKI.sol

Locations

```
1038   path[0] = address(this);
1039   path[1] = uniswapV2Router.WETH();
1040
1041   _approve(address(this), address(uniswapV2Router), tokenAmount);
1042
1043
```

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.