MetaGold Financial

Smart Contract Audit Report

SYSFIXED

30 Jan 2023

TABLE OF CONTENTS

AUDITED DETAILS

Audited Project

Project name	Token ticker	Blockchain
MetaGold Financial	MGF	Binance Smart Chain

Addresses

Contract address	0x1f77f06333B89b94389b9214cA476dd5107Af92a
Contract deployer address	0xdF19f7f9c8179dbf73e752DFcFb247ad4232E416

Project Website

https://t.me/metagoldrewards

Codebase

https://bscscan.com/address/0x1f77f06333B89b94389b9214cA476dd5107Af92a#code

SUMMARY

MetaGold 2.0: The First Digital Gold Certificate of Deposit. MetaGold Financial offers a unique opportunity to experience insane returns with a simple click of a button. This cutting-edge platform, which is the latest iteration of digital gold, provides you with a proven path to high returns on investment. An affiliate program with 10% commission. Stable Coin Staking Utility for income. 75% APY Staking and Blockchain affiliate program.

Contract Summary

Documentation Quality

MetaGold Financial 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 MetaGold Financial with the discovery of several low issues.

Test Coverage

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

Audit Findings Summary

- SWC-101 | It is recommended to use vetted safe math libraries for arithmetic operations consistently on lines 101, 103, 110, 115, 122, 145, 158, 168, 169, 180, 190, 431, 454, 487, 490, 512, 515, 541, 543, 593, 696, 696, 800, 800, 972 and 972.
- 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 855, 856, 857, 901, 902, 903, 986, 987, 988, 1289, 1290, 1302 and 1303.

CONCLUSION

We have audited the MetaGold Financial project released on January 2023 to discover issues and identify potential security vulnerabilities in MetaGold Financial 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 MetaGold Financial 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, and out of bounds array access which the index access expression can cause an exception in case of the use of an invalid array index value.

AUDIT RESULT

Article	Category	Description	Result
Default Visibility	SWC-100 SWC-108	Functions and state variables visibility should be set explicitly. Visibility levels should be specified consciously.	PASS
Integer Overflow and Underflow	SWC-101	If unchecked math is used, all math operations should be safe from overflows and underflows.	ISSUE FOUND
Outdated Compiler Version	SWC-102	It is recommended to use a recent version of the Solidity compiler.	PASS
Floating Pragma	SWC-103	Contracts should be deployed with the same compiler version and flags that they have been tested thoroughly.	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	Sunday Jan 29 2023 12:40:30 GMT+0000 (Coordinated Universal Time)
Finished	Monday Jan 30 2023 23:10:35 GMT+0000 (Coordinated Universal Time)
Mode	Standard
Main Source File	MetaGold.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-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 101

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
100   function mul(int256 a, int256 b) internal pure returns (int256) {
101   int256 c = a * b;
102   require(c != MIN_INT256 || (a & MIN_INT256) != (b & MIN_INT256));
103   require((b == 0) || (c / b == a));
104   return c;
105
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 103

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
102   require(c != MIN_INT256 || (a & MIN_INT256) != (b & MIN_INT256));
103   require((b == 0) || (c / b == a));
104   return c;
105   }
106
107
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 110

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
109   require(b != -1 || a != MIN_INT256);
110   return a / b;
111   }
112
113
114
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 115

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
114   function sub(int256 a, int256 b) internal pure returns (int256) {
115   int256 c = a - b;
116   require((b >= 0 && c <= a) || (b < 0 && c > a));
117   return c;
118   }
119
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 122

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
121   function add(int256 a, int256 b) internal pure returns (int256) {
122   int256 c = a + b;
123   require((b >= 0 && c >= a) || (b < 0 && c < a));
124   return c;
125   }
126
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 145

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
144   function add(uint256 a, uint256 b) internal pure returns (uint256) {
145   uint256 c = a + b;
146   require(c >= a, "SafeMath: addition overflow");
147
148   return c;
149
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 158

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
157   require(b <= a, errorMessage);
158   uint256 c = a - b;
159
160   return c;
161   }
162
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 168

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
167
168   uint256 c = a * b;
169   require(c / a == b, "SafeMath: multiplication overflow");
170
171   return c;
172
```

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 169

low SEVERITY

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

Source File

- MetaGold.sol

Locations

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

SWC-101 | ARITHMETIC OPERATION "/" DISCOVERED

LINE 180

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
179   require(b > 0, errorMessage);
180   uint256 c = a / b;
181   return c;
182   }
183
184
```

SWC-101 | ARITHMETIC OPERATION "%" DISCOVERED

LINE 190

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
189   require(b != 0, errorMessage);
190   return a % b;
191   }
192   }
193
194
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 431

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
430   address owner = _msgSender();
431   _approve(owner, spender, allowance(owner, spender) + addedValue);
432   return true;
433   }
434
435
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 454

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
453   unchecked {
454   _approve(owner, spender, currentAllowance - subtractedValue);
455   }
456
457   return true;
458
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 487

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
486   unchecked {
487   _balances[from] = fromBalance - amount;
488   // Overflow not possible: the sum of all balances is capped by totalSupply, and the
sum is preserved by
489   // decrementing then incrementing.
490   _balances[to] += amount;
491
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 490

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
489   // decrementing then incrementing.
490   _balances[to] += amount;
491   }
492
493   emit Transfer(from, to, amount);
494
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 512

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
511
512   _totalSupply += amount;
513   unchecked {
514   // Overflow not possible: balance + amount is at most totalSupply + amount, which
is checked above.
515   _balances[account] += amount;
516
```

SWC-101 | ARITHMETIC OPERATION "+=" DISCOVERED

LINE 515

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
514   // Overflow not possible: balance + amount is at most totalSupply + amount, which
is checked above.
515   _balances[account] += amount;
516   }
517   emit Transfer(address(0), account, amount);
518
519
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 541

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
540   unchecked {
541   _balances[account] = accountBalance - amount;
542   // Overflow not possible: amount <= accountBalance <= totalSupply.
543   _totalSupply -= amount;
544   }
545
```

SWC-101 | ARITHMETIC OPERATION "-=" DISCOVERED

LINE 543

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
542   // Overflow not possible: amount <= accountBalance <= totalSupply.
543   _totalSupply -= amount;
544   }
545
546   emit Transfer(account, address(0), amount);
547
```

SWC-101 | ARITHMETIC OPERATION "-" DISCOVERED

LINE 593

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
592   unchecked {
593   _approve(owner, spender, currentAllowance - amount);
594   }
595   }
596   }
597
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 696

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
695   uint256 public marketingFee = 10; //1%
696   uint256 public swapTokensAtAmount = 100000 * 10 ** 18;
697   uint256 public burnFee = 10; //1%
698   uint256 public bonusDirectTransaction = 1000; //100%
699   uint256 public bonusSwapTransactionToReferrer = 10; //1%
700
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 696

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
695   uint256 public marketingFee = 10; //1%
696   uint256 public swapTokensAtAmount = 100000 * 10 ** 18;
697   uint256 public burnFee = 10; //1%
698   uint256 public bonusDirectTransaction = 1000; //100%
699   uint256 public bonusSwapTransactionToReferrer = 10; //1%
700
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 800

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
799   _mustDoFee[uniswapV2Pair] = true;
800   _mint(msg.sender, _supply * ( 10 ** decimals()));
801   }
802
803   //to recieve ETH from uniswapV2Router when swaping
804
```

SWC-101 | ARITHMETIC OPERATION "**" DISCOVERED

LINE 800

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
799   _mustDoFee[uniswapV2Pair] = true;
800   _mint(msg.sender, _supply * ( 10 ** decimals()));
801   }
802
803   //to recieve ETH from uniswapV2Router when swaping
804
```

SWC-101 | ARITHMETIC OPERATION "+" DISCOVERED

LINE 972

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
971   require(nr > block.timestamp, "Next rebase must be in near future");
972   require(nr < block.timestamp + 7 *lockpayTwentyFourHours, "Next rebase must be
maximum in 7 days");
973   nextLockpayRebase = nr;
974   }
975
976
```

SWC-101 | ARITHMETIC OPERATION "*" DISCOVERED

LINE 972

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
971   require(nr > block.timestamp, "Next rebase must be in near future");
972   require(nr < block.timestamp + 7 *lockpayTwentyFourHours, "Next rebase must be
maximum in 7 days");
973   nextLockpayRebase = nr;
974   }
975
976
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 855

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
854   address[] memory path = new address[](2);
855   path[0] = bnb_address;
856   path[1] = meta_address;
857   uint256 minamount = uniswapV2Router.getAmountsOut(msg.value, path)[1];
858   uint256 origAmount = minamount;
859
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 856

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
855   path[0] = bnb_address;
856   path[1] = meta_address;
857   uint256 minamount = uniswapV2Router.getAmountsOut(msg.value, path)[1];
858   uint256 origAmount = minamount;
859   uint256 reward = minamount.mul(bonusSwapTransactionToReferrer).div(1000);
860
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 857

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
856   path[1] = meta_address;
857   uint256 minamount = uniswapV2Router.getAmountsOut(msg.value, path)[1];
858   uint256 origAmount = minamount;
859   uint256 reward = minamount.mul(bonusSwapTransactionToReferrer).div(1000);
860   if( referral == msg.sender) {
861
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 901

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
900   address[] memory path = new address[](2);
901   path[0] = bnb_address;
902   path[1] = meta_address;
903   uint256 minamount = uniswapV2Router.getAmountsOut(amount, path)[1];
904
905
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 902

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
901   path[0] = bnb_address;
902   path[1] = meta_address;
903   uint256 minamount = uniswapV2Router.getAmountsOut(amount, path)[1];
904
905   rewardReferrer = 0;
906
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 903

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
902   path[1] = meta_address;
903   uint256 minamount = uniswapV2Router.getAmountsOut(amount, path)[1];
904
905   rewardReferrer = 0;
906   if( referral != address(0)) {
907
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 986

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
985   address[] memory path = new address[](2);
986   path[0] = bnb_address;
987   path[1] = meta_address;
988   return uniswapV2Router.getAmountsOut(inAmount, path)[1];
989   }
990
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 987

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
986   path[0] = bnb_address;
987   path[1] = meta_address;
988   return uniswapV2Router.getAmountsOut(inAmount, path)[1];
989   }
990
991
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 988

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
987   path[1] = meta_address;
988   return uniswapV2Router.getAmountsOut(inAmount, path)[1];
989   }
990
991   /**
992
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1289

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
1288   address[] memory path = new address[](2);
1289   path[0] = address(this);
1290   path[1] = uniswapV2Router.WETH();
1291
1292   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
1293
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1290

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
1289   path[0] = address(this);
1290   path[1] = uniswapV2Router.WETH();
1291
1292   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
1293   tokenAmount,
1294
```

SWC-110 | OUT OF BOUNDS ARRAY ACCESS

LINE 1302

low SEVERITY

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

Source File

- MetaGold.sol

Locations

```
1301   address[] memory path = new address[](2);
1302   path[0] = address(this);
1303   path[1] = uniswapV2Router.WETH();
1304
1305   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
1306
```

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

- MetaGold.sol

Locations

```
1302   path[0] = address(this);
1303   path[1] = uniswapV2Router.WETH();
1304
1305   uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(
1306   tokenAmount,
1307
```

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.