Cyberscope

Audit Report

DigiToken

April 2024

Network BSC

Address 0x2f8687013ca06a033e33b423E8533E8dF0625e15

Audited by © cyberscope

Analysis

Critical Medium Minor / Informative Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Unresolved
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	MT	Mints Tokens	Passed
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Unresolved

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	AOI	Arithmetic Operations Inconsistency	Unresolved
	CO	Code Optimization	Unresolved
	MEE	Missing Events Emission	Unresolved
	PAMAR	Pair Address Max Amount Restriction	Unresolved
	PMRM	Potential Mocked Router Manipulation	Unresolved
	RRS	Redundant Require Statement	Unresolved
	RSML	Redundant SafeMath Library	Unresolved
	RSW	Redundant Storage Writes	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved

Table of Contents

Review

Contract Name	DigiFolioToken
Compiler Version	v0.8.21+commit.d9974bed
Optimization	200 runs
Explorer	https://bscscan.com/address/0x2f8687013ca06a033e33b423e8533e8df0625e15
Address	0x2f8687013ca06a033e33b423e8533e8df0625e15
Network	BSC
Symbol	DGFL
Decimals	8
Total Supply	500,000,000
Badge Eligibility	Must Fix Criticals

Audit Updates

Initial Audit	30 Apr 2024

Source Files

Filename	SHA256
DigiFolioToken.sol	c9da076c40b1fd384291e40bfacb95f081ef2b9ba8b6e147619b144fc10aa68f

Findings Breakdown

Critical	2
Medium	0
Minor / Informative	9

Severity	Unresolved	Acknowledged	Resolved	Other
Critical	2	0	0	0
Medium	0	0	0	0
Minor / Informative	9	0	0	0

ST - Stops Transactions

Criticality	Critical
Location	DigiFolioToken.sol#L290,304
Status	Unresolved

Description

Initially, the transactions are disabled for all users except the contract owner. The contract owner has to call the `enableTrading` function. Furthermore, the owner has the authority to stop the transactions for users by seeting the `maxHoldLimit` to a very low value. Lastly, the owner has the authority to stop the transactions as described in the PAMAR finding. As a result, the contract may operate as a honeypot.

```
require(tradingActive, "Trading not started yet");

function enableTrading(address router, address pair) external
onlyOwner {
        tradingActive = true;
        uniswapRouter = IUniswapV2Router02(router);
        uniswapV2Pair = pair;
        _isExcludedFromLimit[router] = true;
        _isExcludedFromLimit[pair] = true;
    }

require(
  balanceOf(to) + amount  <= maxHoldLimit,
  "Max holding limit exceeds"
);

function setMaxHoldingLimit(uint256 _maxHoldLimit) external
onlyOwner {
        maxHoldLimit = _maxHoldLimit;
    }
```

Recommendation

The contract could embody a check for not allowing setting the `maxHoldLimit` less than a reasonable amount. A suggested implementation could check that the minimum amount should be more than a fixed percentage of the total supply. The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

BC - Blacklists Addresses

Criticality	Critical
Location	DigiFolioToken.sol#L286,324
Status	Unresolved

Description

The contract owner has the authority to stop addresses from transactions. The owner may take advantage of it by calling the `includeOrExcludeFromBlacklist` function.

```
require(
  !_isBlacklisted[from] && !_isBlacklisted[to],
  "Address blacklisted"
);

function includeOrExcludeFromBlacklist(address _addr, bool
_state)
      external
      onlyOwner
  {
      _isBlacklisted[_addr] = _state;
  }
```

Recommendation

The team should carefully manage the private keys of the owner’s account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

AOI - Arithmetic Operations Inconsistency

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L295,311,312
Status	Unresolved

Description

The contract uses both the SafeMath library and native arithmetic operations. The SafeMath library is commonly used to mitigate vulnerabilities related to integer overflow and underflow issues. However, it was observed that the contract also employs native arithmetic operators (such as +, -, *, /) in certain sections of the code.

The combination of SafeMath library and native arithmetic operations can introduce inconsistencies and undermine the intended safety measures. This discrepancy creates an inconsistency in the contract's arithmetic operations, increasing the risk of unintended consequences such as inconsistency in error handling, or unexpected behavior.

```
_balances[from] = _balances[from].sub(amount);
_balances[to] = _balances[to].add(amount);

balanceOf(to) + amount <= maxHoldLimit
```

Recommendation

To address this finding and ensure consistency in arithmetic operations, it is recommended to standardize the usage of arithmetic operations throughout the contract. The contract should be modified to either exclusively use SafeMath library functions or entirely rely on native arithmetic operations, depending on the specific requirements and design considerations. This consistency will help maintain the contract's integrity and mitigate potential vulnerabilities arising from inconsistent arithmetic operations.

CO - Code Optimization

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L347
Status	Unresolved

Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations. Specifically, The function `burn` performs the burning functionality even if zero amount is provided. Furthermore, there is a redundant check that the `msg.sender` is not the zero address that cannot happen.

```
function burn(uint256 amount) external onlyOwner {
    require(msg.sender != address(0), "ERC20: burn from the
zero address");
    uint256 accountBalance = _balances[msg.sender];
    require(accountBalance >= amount, "ERC20: burn amount
exceeds balance");
    unchecked {
        _balances[msg.sender] = accountBalance - amount;
        _tTotal -= amount;
    }
    emit Transfer(msg.sender, address(0), amount);
}
```

Recommendation

The team is advised to take these segments into consideration and rewrite them so the runtime will be more performant. That way it will improve the efficiency and performance of the source code and reduce the cost of executing it.

MEE - Missing Events Emission

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L316,324,331,338
Status	Unresolved

Description

The contract performs actions and state mutations from external methods that do not result in the emission of events. Emitting events for significant actions is important as it allows external parties, such as wallets or dApps, to track and monitor the activity on the contract. Without these events, it may be difficult for external parties to accurately determine the current state of the contract.

```
function enableTrading(address router, address pair) external
onlyOwner {
    tradingActive = true;
    uniswapRouter = IUniswapV2Router02(router);
    uniswapV2Pair = pair;
    _isExcludedFromLimit[router] = true;
    _isExcludedFromLimit[pair] = true;
}

function setMaxHoldingLimit(uint256 _maxHoldLimit) external
onlyOwner {
    maxHoldLimit = _maxHoldLimit;
}
```

Recommendation

It is recommended to include events in the code that are triggered each time a significant action is taking place within the contract. These events should include relevant details such as the user's address and the nature of the action taken. By doing so, the contract will be more transparent and easily auditable by external parties. It will also help prevent potential issues or disputes that may arise in the future.

PAMAR - Pair Address Max Amount Restriction

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L294,304
Status	Unresolved

Description

The contract is configured to enforce a maximum token accumulation limit through checks. This mechanism aims to prevent excessive token concentration by reverting transactions that overcome the specified cap. However, this functionality encounters issues when transactions default to the pair address during sales. If the pair address is not listed in the exceptions, then the sale transactions are inadvertently stopped, effectively disrupting operations and making the contract susceptible to unintended behaviors akin to a honeypot.

```
require(
    balanceOf(to) + amount  <= maxHoldLimit,
    "Max holding limit exceeds"
);
```

Recommendation

It is advised to modify the contract to ensure uninterrupted operations by either permitting the pair address to exceed the established token accumulation limit or by safeguarding its status in the exception list. By recognizing and allowing these essential addresses the flexibility to hold more tokens than typical limits, the contract can maintain seamless transaction flows and uphold the liquidity and stability of the ecosystem. This modification is vital for avoiding disruptions that could impact the functionality and security of the contract.

PMRM - Potential Mocked Router Manipulation

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L316
Status	Unresolved

Description

The contract does not have a check to ensure that the `enableTrading` function can be called only once. As a result, this function can allows the owner to modify the router address and create a new pair. While this feature provides flexibility, it introduces a security threat. The owner could set the router address to any contract that implements the router's interface, potentially containing malicious code. In the event of a transaction triggering the swap functionality with such a malicious contract as the router, the transaction may be manipulated.

```
function enableTrading(address router, address pair) external
onlyOwner {
    tradingActive = true;
    uniswapRouter = IUniswapV2Router02(router);
    uniswapV2Pair = pair;
    _isExcludedFromLimit[router] = true;
    _isExcludedFromLimit[pair] = true;
}
```

Recommendation

It is recommended a check be enforced, that allows the `openTrading` function to be called only once. Furthermore, the team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions.

Temporary Solutions:

These measurements do not decrease the severity of the finding

- Introduce a time-locker mechanism with a reasonable delay.
- Introduce a multi-signature wallet so that many addresses will confirm the action.
- Introduce a governance model where users will vote about the actions.

Permanent Solution:

- Renouncing the ownership, which will eliminate the threats but it is non-reversible.

RRS - Redundant Require Statement

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L45
Status	Unresolved

Description

The contract utilizes a `require` statement within the `add` function aiming to prevent overflow errors. This function is designed based on the SafeMath library's principles. In Solidity version 0.8.0 and later, arithmetic operations revert on overflow and underflow, making the overflow check within the function redundant. This redundancy could lead to extra gas costs and increased complexity without providing additional security.

```
function add(uint256 a, uint256 b) internal pure returns
(uint256) {
      uint256 c = a + b;
      require(c >= a, "SafeMath: addition overflow");
      return c;
}
```

Recommendation

It is recommended to remove the `require` statement from the add function since the contract is using a Solidity pragma version equal to or greater than 0.8.0. By doing so, the contract will leverage the built-in overflow and underflow checks provided by the Solidity language itself, simplifying the code and reducing gas consumption. This change will uphold the contract's integrity in handling arithmetic operations while optimizing for efficiency and cost-effectiveness.

RSML - Redundant SafeMath Library

Criticality	Minor / Informative
Location	DigiFolioToken.sol
Status	Unresolved

Description

SafeMath is a popular Solidity library that provides a set of functions for performing common arithmetic operations in a way that is resistant to integer overflows and underflows.

Starting with Solidity versions that are greater than or equal to 0.8.0, the arithmetic operations revert to underflow and overflow. As a result, the native functionality of the Solidity operations replaces the SafeMath library. Hence, the usage of the SafeMath library adds complexity, overhead and increases gas consumption unnecessarily in cases where the explanatory error message is not used.

```
library SafeMath {...}
```

Recommendation

The team is advised to remove the SafeMath library in cases where the revert error message is not used. Since the version of the contract is greater than `0.8.0` then the pure Solidity arithmetic operations produce the same result.

If the previous functionality is required, then the contract could exploit the `unchecked { ... }` statement.

Read more about the breaking change on https://docs.soliditylang.org/en/v0.8.16/080-breaking-changes.html#solidity-v0-8-0-breaking-changes.

RSW - Redundant Storage Writes

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L316,324,331,338
Status	Unresolved

Description

The contract modifies the state of the following variables without checking if their current value is the same as the one given as an argument. As a result, the contract performs redundant storage writes, when the provided parameter matches the current state of the variables, leading to unnecessary gas consumption and inefficiencies in contract execution.

```
function includeOrExcludeFromBlacklist(address _addr, bool
_state)
    external
    onlyOwner
{
    _isBlacklisted[_addr] = _state;
}

function includeOrExcludeFromLimit(address _addr, bool _state)
    external
    onlyOwner
{
    _isExcludedFromLimit[_addr] = _state;
}
```

Recommendation

The team is advised to implement additional checks within to prevent redundant storage writes when the provided argument matches the current state of the variables. By incorporating statements to compare the new values with the existing values before proceeding with any state modification, the contract can avoid unnecessary storage operations, thereby optimizing gas usage.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	DigiFolioToken.sol#L169,176,177,179,181,186,187,324,331,338
Status	Unresolved

Description

The Solidity style guide is a set of guidelines for writing clean and consistent Solidity code. Adhering to a style guide can help improve the readability and maintainability of the Solidity code, making it easier for others to understand and work with.

The followings are a few key points from the Solidity style guide:

1. Use camelCase for function and variable names, with the first letter in lowercase (e.g., myVariable, updateCounter).
2. Use PascalCase for contract, struct, and enum names, with the first letter in uppercase (e.g., MyContract, UserStruct, ErrorEnum).
3. Use uppercase for constant variables and enums (e.g., MAX_VALUE, ERROR_CODE).
4. Use indentation to improve readability and structure.
5. Use spaces between operators and after commas.
6. Use comments to explain the purpose and behavior of the code.
7. Keep lines short (around 120 characters) to improve readability.

```
function WETH() external pure returns (address);
mapping(address => bool) public _isExcludedFromLimit
mapping(address => bool) public _isBlacklisted
uint256 public _buyCount = 0
uint8 private constant _decimals = 8
string private constant _name = "DigiToken"
string private constant _symbol = "DGFL"
bool _state
address _addr
uint256 _maxHoldLimit
```

Recommendation

By following the Solidity naming convention guidelines, the codebase increased the readability, maintainability, and makes it easier to work with.
Find more information on the Solidity documentation
https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention.

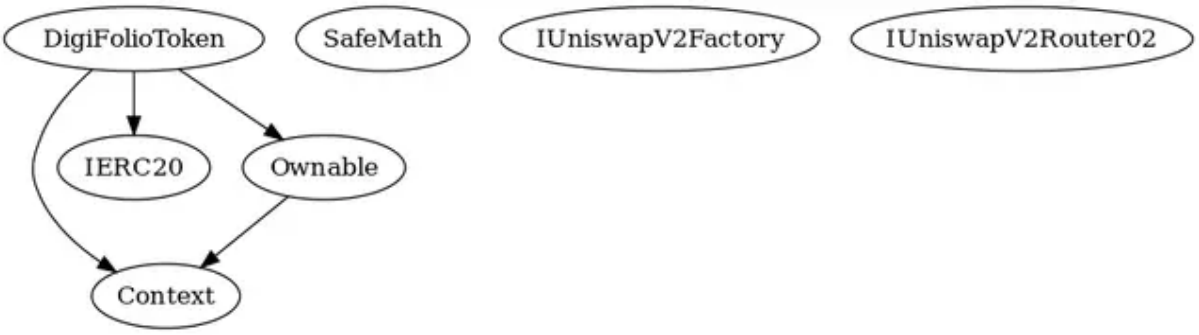
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		

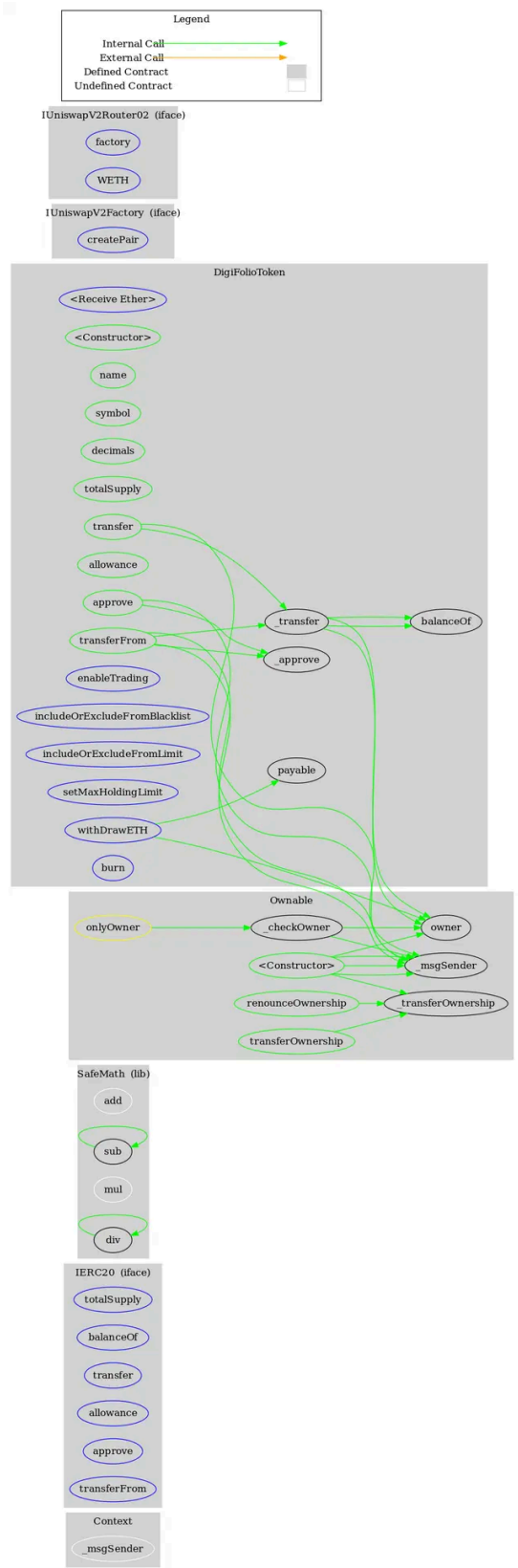
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
IUniswapV2Factory	Interface			
	createPair	External	✓	-
IUniswapV2Router02	Interface			
	factory	External		-
	WETH	External		-
DigiFolioToken	Implementation	Context, IERC20, Ownable		
		External	Payable	-
		Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-

	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	_approve	Private	✓	
	_transfer	Private	✓	
	enableTrading	External	✓	onlyOwner
	includeOrExcludeFromBlacklist	External	✓	onlyOwner
	includeOrExcludeFromLimit	External	✓	onlyOwner
	setMaxHoldingLimit	External	✓	onlyOwner
	withDrawETH	External	✓	onlyOwner
	burn	External	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IUniswapV2Router02 (iface)
factory
WETH
IUniswapV2Factory (iface)
createPair
DigiFolioToken
<Receive Ether>
<Constructor>
name
symbol
decimals
totalSupply
transfer
allowance
approve
transferFrom
enableTrading
includeOrExcludeFromBlacklist
includeOrExcludeFromLimit
setMaxHoldingLimit
withDrawETH
burn
_transfer
balanceOf
_approve
payable
Ownable
onlyOwner
_checkOwner
owner
<Constructor>
msgSender
renounceOwnership
transferOwnership
transferOwnership
SafeMath (lib)
add
sub
mul
div
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
Context
_msgSender

Summary

DigiToken contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. There are some functions that can be abused by the owner like stop transactions and massively blacklist addresses. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. 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 Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment 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.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope's goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io