



Cyberscope

Audit Report

Tectum Emission Token

March 2023

SHA256 9da16aa826451f964e6eb156100c0d5238c98a2a23298bdb7910fa2b9b790cee

Audited by © cyberscope

Table of Contents

Table of Contents	1
Review	2
Audit Updates	2
Source Files	2
Analysis	3
MT - Mints Tokens	4
Description	4
Recommendation	5
Diagnostics	6
R11 - Redundant Inheritance Issue	7
Description	7
Recommendation	7
L04 - Conformance to Solidity Naming Conventions	8
Description	8
Recommendation	9
L19 - Stable Compiler Version	10
Description	10
Recommendation	10
L23 - ERC20 Interface Misuse	11
Description	11
Recommendation	11
Team Update	12
Functions Analysis	13
Inheritance Graph	16
Flow Graph	17
Summary	18
Disclaimer	19
About Cyberscope	20

Review

Audit Updates

Initial Audit	09 Mar 2023 https://github.com/cyberscope-io/audits/tree/main/2-tet/v1/audit.pdf
Corrected Phase 2	14 Mar 2023

Source Files

Filename	SHA256
TetToken.sol	9da16aa826451f964e6eb156100c0d523 8c98a2a23298bdb7910fa2b9b790cee

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

Severity	Code	Description	Status
●	ST	Stops Transactions	Passed
●	OCTD	Transfers Contract's Tokens	Passed
●	OTUT	Transfers User's Tokens	Passed
●	ELFM	Exceeds Fees Limit	Passed
●	ULTW	Transfers Liquidity to Team Wallet	Passed
●	MT	Mints Tokens	Unresolved
●	BT	Burns Tokens	Passed
●	BC	Blacklists Addresses	Passed

MT - Mints Tokens

Criticality	Critical
Location	TetToken.sol#L291,315
Status	Unresolved

Description

The contract owner has the authority to mint tokens. The owner may take advantage of it by calling the `TETwrite` or `issue` function. As a result, the contract tokens will be highly inflated.

```
function TETwrite(uint newTS) public onlyOwner returns (uint) {
    require( newTS <= MAX_TET);
    require( newTS != _totalSupply);

    if (newTS > _totalSupply) {
        balances[owner] = balances[owner].add(newTS - _totalSupply);
        _totalSupply = newTS ;
    } else {
        require (balances[owner] >= ( _totalSupply - newTS ));
        balances[owner] = balances[owner].sub(_totalSupply - newTS) ;
        _totalSupply = newTS ;
    }
    TETwriteEvent(_totalSupply);
    return _totalSupply ;
}
...
function issue(uint amount) public onlyOwner {
    require(_totalSupply + amount <= MAX_TET);
    require(_totalSupply + amount > _totalSupply);
    require(balances[owner] + amount > balances[owner]);

    balances[owner] += amount;
    _totalSupply += amount;
    Issue(amount);
}
```

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. Some suggestions are:

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

Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	R11	Redundant Inheritance Issue	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved
●	L19	Stable Compiler Version	Unresolved
●	L23	ERC20 Interface Misuse	Acknowledged

RII - Redundant Inheritance Issue

Criticality	Minor / Informative
Location	TetToken.sol#L93,232
Status	Unresolved

Description

The contract includes the Pausable and BlackList contracts, but it does not make use of their functionalities.

```
contract Pausable is Ownable { ... }  
contract BlackList is Ownable, BasicToken {
```

Recommendation

The Inheritance of unused contracts in the contract implementation should be avoided. It is recommended to remove unused contracts.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	TetToken.sol#L52,71,156,168,188,205,223,235,245,250,287,291
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.

```
address _owner
uint public _totalSupply
uint _value
address _to
address _from
address _spender
address _maker
address _evilUser
address _clearedUser

function TETRead() public constant returns (uint) {
    return _totalSupply;
}

...
```

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>.

L19 - Stable Compiler Version

Criticality	Minor / Informative
Location	TetToken.sol#L1
Status	Unresolved

Description

The `^` symbol indicates that any version of Solidity that is compatible with the specified version (i.e., any version that is a higher minor or patch version) can be used to compile the contract. The version lock is a mechanism that allows the author to specify a minimum version of the Solidity compiler that must be used to compile the contract code. This is useful because it ensures that the contract will be compiled using a version of the compiler that is known to be compatible with the code.

```
pragma solidity ^0.4.17;
```

Recommendation

The team is advised to lock the pragma to ensure the stability of the codebase. The locked pragma version ensures that the contract will not be deployed with an unexpected version. An unexpected version may produce vulnerabilities and undiscovered bugs. The compiler should be configured to the lowest version that provides all the required functionality for the codebase. As a result, the project will be compiled in a well-tested LTS (Long Term Support) environment.

L23 - ERC20 Interface Misuse

Criticality	Minor / Informative
Location	TetToken.sol#L74,84,85,156,188,205
Status	Acknowledged

Description

The ERC20 is a standard interface for tokens on the blockchain. It defines a set of functions and events that a contract must implement in order to be considered an ERC20 token. According to the ERC20 interface, the transfer function returns a bool value, which indicates the success or failure of the transfer. If the transfer is successful, the function returns true. If the transfer fails, the function returns false. The contract implements the transfer function without the return value.

```
function transfer(address to, uint value) public;
function transferFrom(address from, address to, uint value) public;
function approve(address spender, uint value) public;

function transfer(address _to, uint _value) public onlyPayloadSize(2 * 32)
whenNotPaused {
    require (!(_to == 0x0));
    balances[msg.sender] = balances[msg.sender].sub(_value);
    balances[_to] = balances[_to].add(_value);
    Transfer(msg.sender, _to, _value);
}

...
```

Recommendation

The incorrect implementation of the ERC20 interface could potentially lead to problems when interacting with the contract, as other contracts or applications that expect the ERC20 interface may not behave as expected.

Team Update

The team responded with the following statement:

“Partially agree with the statement however the same tether SC has proven to be stable with the time”

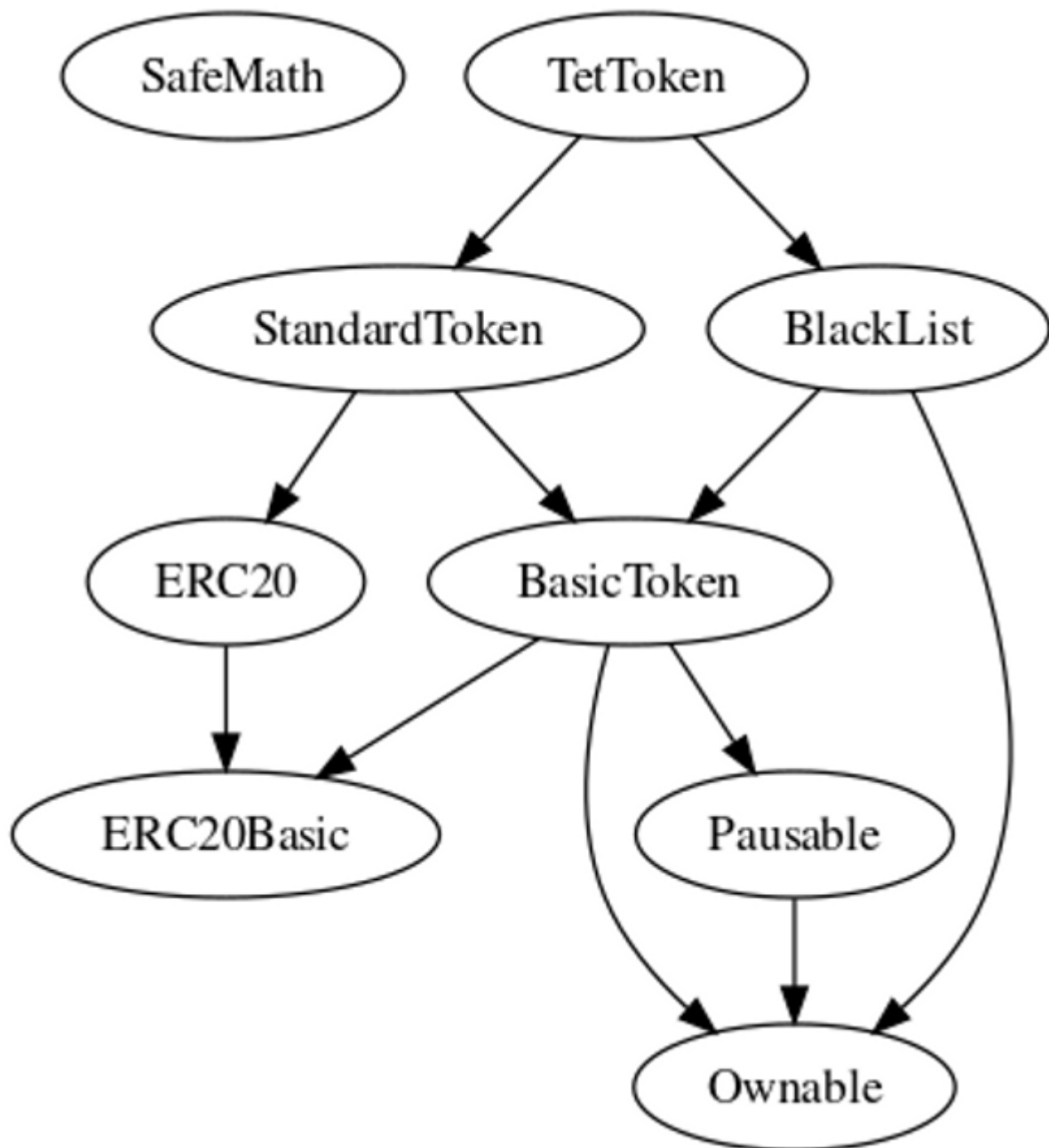
Functions Analysis

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
Ownable	Implementation			
		Public	✓	-
	changeOwner	Public	✓	onlyOwner
	confirmOwner	Public	✓	-
ERC20Basic	Implementation			
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
ERC20	Implementation	ERC20Basic		
	allowance	Public		-
	transferFrom	Public	✓	-
	approve	Public	✓	-
Pausable	Implementation	Ownable		
	pause	Public	✓	onlyOwner whenNotPaused

	unpause	Public	✓	onlyOwner whenPaused
BasicToken	Implementation	Ownable, Pausable, ERC20Basic		
	transfer	Public	✓	onlyPayloadSize whenNotPaused
	balanceOf	Public		-
StandardToken	Implementation	BasicToken, ERC20		
	transferFrom	Public	✓	onlyPayloadSize whenNotPaused
	approve	Public	✓	onlyPayloadSize
	allowance	Public		-
BlackList	Implementation	Ownable, BasicToken		
	getBlackListStatus	External		-
	getOwner	External		-
	addBlackList	Public	✓	onlyOwner
	removeBlackList	Public	✓	onlyOwner
TetToken	Implementation	StandardToken, BlackList		
		Public	✓	-
	totalSupply	Public		-
	TETRead	Public		-
	TETwrite	Public	✓	onlyOwner
	issue	Public	✓	onlyOwner

	redeem	Public	✓	onlyOwner
--	--------	--------	---	-----------

Inheritance Graph



Flow Graph



Summary

Tectum Emission Token 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 mint tokens. If the contract owner abuses the mint functionality, then the contract will be highly inflated. 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>