Cyberscope

Audit Report

Virtual Versions

Aug 2023

Network	ETH
Address	0x7556a1ed241bc4b56530c8e8e1347629c8884f23
Audited by	© cyberscope

Analysis

● Critical ● Medium ● Minor / Informative ● Pass

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

Diagnostics

🔴 Critical 🟠 Medium ⚪ Minor / Informative

Severity	Code	Description	Status
🔴	US	Untrusted Source	Unresolved
⚪	PUFC	Potential Unauthorized Function Call	Unresolved
⚪	MC	Missing Check	Unresolved
⚪	MFN	Misleading Function Naming	Unresolved
⚪	MEE	Missing Events Emission	Unresolved
⚪	IDI	Immutable Declaration Improvement	Unresolved
⚪	L04	Conformance to Solidity Naming Conventions	Unresolved
⚪	L16	Validate Variable Setters	Unresolved

Table of Contents

Analysis **1**
Diagnostics **2**
Table of Contents **3**
Review **4**
Audit Updates 4
Source Files 4
Findings Breakdown **5**
US - Untrusted Source 6
Description 6
Recommendation 6
PUFC - Potential Unauthorized Function Call 7
Description 7
Recommendation 7
MC - Missing Check 8
Description 8
Recommendation 8
MFN - Misleading Function Naming 9
Description 9
Recommendation 9
MEE - Missing Events Emission 10
Description 10
Recommendation 10
IDI - Immutable Declaration Improvement 11
Description 11
Recommendation 11
L04 - Conformance to Solidity Naming Conventions 12
Description 12
Recommendation 12
L16 - Validate Variable Setters 13
Description 13
Recommendation 13
Functions Analysis **14**
Inheritance Graph **16**
Flow Graph **17**
Summary **18**
Disclaimer **19**
About Cyberscope **20**

Review

Contract Name	Erc20Token
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Explorer	https://etherscan.io/address/0x7556a1ed241bc4b56530c8e8e1347629c8884f23
Address	0x7556a1ed241bc4b56530c8e8e1347629c8884f23
Network	ETH
Symbol	VV
Decimals	18
Total Supply	1,000,000,000

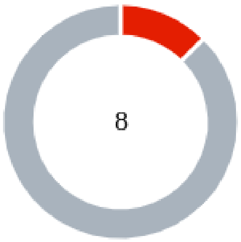
Audit Updates

Initial Audit	06 Aug 2023

Source Files

Filename	SHA256
Erc20Token.sol	96d9d881a01e72d7377c36c374c3e686b6277c5f3a9cf3d9358746cfd4548b21

Findings Breakdown



●	Critical	1
●	Medium	0
●	Minor / Informative	7

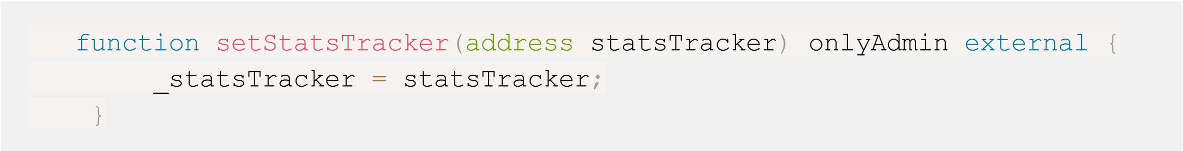
Severity	Unresolved	Acknowledged	Resolved	Other
● Critical	1	0	0	0
● Medium	0	0	0	0
● Minor / Informative	7	0	0	0

US - Untrusted Source

Criticality	Critical
Location	Erc20Token.sol#L198
Status	Unresolved

Description

The contract uses an external contract in order to determine the transaction's flow. The external contract is untrusted. As a result, it may produce security issues and harm the transactions.



```
    function setStatsTracker(address statsTracker) onlyAdmin external {
        _statsTracker = statsTracker;
    }
```

Recommendation

The contract should use a trusted external source. A trusted source could be either a commonly recognized or an audited contract. The pointing addresses should not be able to change after the initialization.

PUFC - Potential Unauthorized Function Call

Criticality	Minor / Informative
Location	Erc20Token.sol#L191
Status	Unresolved

Description

The contract contains the `confirmNewAdmin` function that can be called by the `onlyAdminCandidate`. This function allows the `_adminCandidate` to set its address as the `_admin` address. As a result, the `_adminCandidate` can call the `confirmNewAdmin` function and set its address as the `_admin` address, thereby gaining the privileges of the admin address. This could potentially lead to a situation where the `_adminCandidate` could gain unauthorized control over the contract. This is a significant security concern as it could lead to misuse of the contract and potentially compromise the integrity and security of the contract.

```
   function confirmNewAdmin() onlyAdminCandidate external {
        emit AdminChangeConfirmed(_admin, _adminCandidate);
        _admin = _adminCandidate;
        _adminCandidate = address(0);
    }
```

Recommendation

It is recommended to reconsider who can call the `confirmNewAdmin` function. If the intended purpose is for the admin to call it, then the `onlyAdmin` modifier should be used instead of the `onlyAdminCandidate` modifier. This change will ensure that only the current admin can confirm and set a new admin address, thereby preventing potential unauthorized access and control over the contract. This will enhance the security and integrity of the contract.

MC - Missing Check

Criticality	Minor / Informative
Location	Erc20Token.sol#L186
Status	Unresolved

Description

The contract is processing variables that have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

The contract contains the `changeAdmin` function which is used to change an address to a new address. However, there is no check in place to validate that the new address being passed as `adminCandidate` is not the zero address. This lack of validation could potentially lead to inadvertent assignment of the zero address as the `adminCandidate`, which could have serious implications for the contract's functionality and security.

The contract does contain a function `_ensureNotZeroAddress` which requires an address not to be zero. However, this function is not being utilized in the `changeAdmin` function to ckeck the `adminCandidate` address.

```
function changeAdmin(address adminCandidate) onlyAdmin external {
     _adminCandidate = adminCandidate;
     emit AdminChangeRequested(_admin, adminCandidate);
 }
```

Recommendation

The team is advised to properly check the variables according to the required specifications. It is recommended to integrate the `_ensureNotZeroAddress` function within the `changeAdmin` function to ensure that the `adminCandidate` address is not the zero address.

MFN - Misleading Function Naming

Criticality	Minor / Informative
Location	Erc20Token.sol#L186
Status	Unresolved

Description

Functions can have misleading names, if their names do not accurately reflect their implementation or the purpose they serve. The contract contains the `changeAdmin` function whose name is misleading as to its actual implementation. The function name suggests that it would change the admin address of the contract. However, the function does not directly change the admin address. Instead, it sets the `adminCandidate` address. This discrepancy between the function name and its actual operation can lead to confusion and misinterpretation of the contract's functionality. It is crucial for the function names to accurately represent their operations to ensure code readability and maintainability.

```
    function changeAdmin(address adminCandidate) onlyAdmin external {
        _adminCandidate = adminCandidate;
        emit AdminChangeRequested(_admin, adminCandidate);
    }
```

Recommendation

It's always a good practice for the contract to contain function names that are specific and descriptive. It is recommended to rename the `changeAdmin` function to a more descriptive and accurate name, to indicate that the function is used to set the `adminCandidate` address rather than directly changing the `admin` address. This change will improve the clarity of the code and reduce potential misunderstandings about the function's purpose and operation. It will also align the function name with its actual implementation, enhancing the overall readability and maintainability of the smart contract.

MEE - Missing Events Emission

Criticality	Minor / Informative
Location	Erc20Token.sol#L198
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 setStatsTracker(address statsTracker) onlyAdmin external {
         _statsTracker = statsTracker;
    }
```

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.

IDI - Immutable Declaration Improvement

Criticality	Minor / Informative
Location	Erc20Token.sol#L163,164,165
Status	Unresolved

Description

The contract declares state variables that their value is initialized once in the constructor and are not modified afterwards. The `immutable` is a special declaration for this kind of state variables that saves gas when it is defined.

```
_name
_symbol
_decimals
```

Recommendation

By declaring a variable as immutable, the Solidity compiler is able to make certain optimizations. This can reduce the amount of storage and computation required by the contract, and make it more gas-efficient.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	Erc20Token.sol#L139,140,141
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 public _admin
address public _adminCandidate
address public _statsTracker
```

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.

L16 - Validate Variable Setters

Criticality	Minor / Informative
Location	Erc20Token.sol#L161,169,183,194
Status	Unresolved

Description

The contract performs operations on variables that have been configured on user-supplied input. These variables are missing of proper check for the case where a value is zero. This can lead to problems when the contract is executed, as certain actions may not be properly handled when the value is zero.

```
_admin = admin_
_statsTracker = statsTracker_
_adminCandidate = adminCandidate
_statsTracker = statsTracker
```

Recommendation

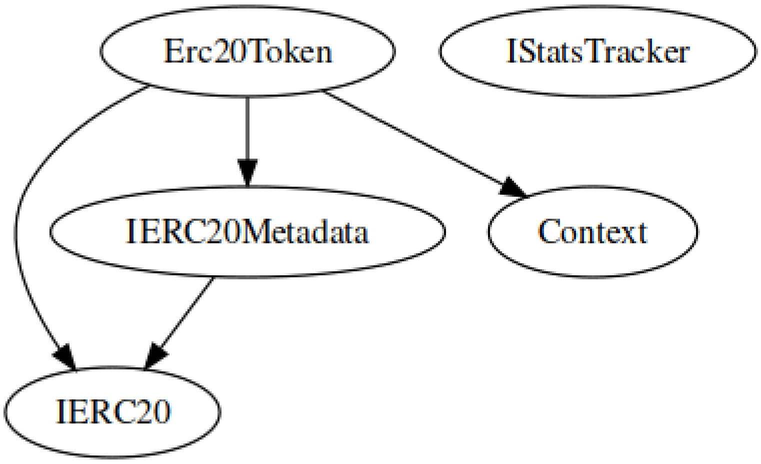
By adding the proper check, the contract will not allow the variables to be configured with zero value. This will ensure that the contract can handle all possible input values and avoid unexpected behavior or errors. Hence, it can help to prevent the contract from being exploited or operating unexpectedly.

Functions Analysis

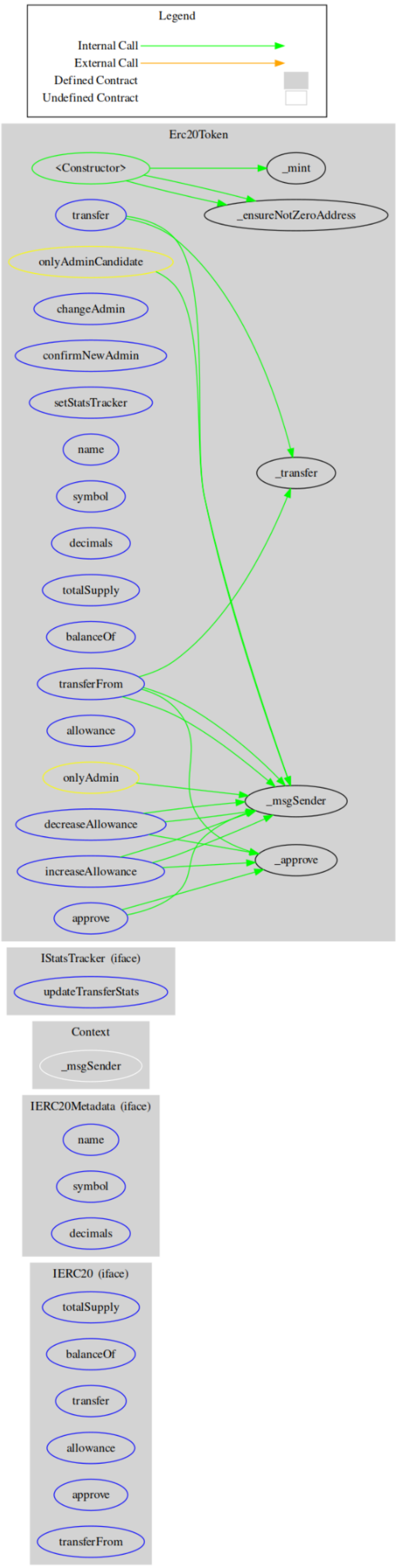
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
Context	Implementation			
	_msgSender	Internal		
IStatsTracker	Interface			
	updateTransferStats	External	✓	-

Erc20Token	Implementation	Context, IERC20, IERC20Metadata		
		Public	✓	-
	changeAdmin	External	✓	onlyAdmin
	confirmNewAdmin	External	✓	onlyAdminCandidate
	setStatsTracker	External	✓	onlyAdmin
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
	increaseAllowance	External	✓	-
	decreaseAllowance	External	✓	-
	_transfer	Private	✓	
	_mint	Private	✓	
	_approve	Private	✓	
	_ensureNotZeroAddress	Private		

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Erc20Token
<Constructor>
_mint
_ensureNotZeroAddress
transfer
onlyAdminCandidate
changeAdmin
confirmNewAdmin
setStatsTracker
name
symbol
decimals
totalSupply
balanceOf
_transfer
transferFrom
allowance
onlyAdmin
_msgSender
decreaseAllowance
_approve
increaseAllowance
approve
IStatsTracker (iface)
updateTransferStats
Context
_msgSender
IERC20Metadata (iface)
name
symbol
decimals
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom

Summary

Virtual Versions contract implements a token mechanism. This audit investigates security issues, business logic concerns and potential improvements. Virtual Versions is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner has access to an external contract. If the owner’s credentials copromized, then the contract could stop the transactions or transform the token into a honeypot.

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