Cyberscope

Audit Report

R-DEE Protocol

March 2024

Network	ETH
Address	0xe4cbd3ff926796e6e95e81f1268258418a0c5cda
Audited by	© cyberscope

Table of Contents

Review

Contract Name	RDGXToken
Compiler Version	v0.8.21+commit.d9974bed
Optimization	200 runs
Explorer	https://etherscan.io/address/0xe4cbd3ff926796e6e95e81f1268258418a0c5cda
Address	0xe4cbd3ff926796e6e95e81f1268258418a0c5cda
Network	ETH
Symbol	RDGX
Decimals	18
Total Supply	1,000,000,000

Audit Updates

Initial Audit	01 Mar 2024

Source Files

Filename	SHA256
contracts/RDGXToken.sol	6a9b086bb470ac359d6a54dede7a3712811b93494d04c1cd00cebf4ccef322df
@openzeppelin/contracts/utils/Strings.sol	cb2df477077a5963ab50a52768cb74ec6f32177177a78611ddbbe2c07e2d36de
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a

@openzeppelin/contracts/utils/structs/EnumerableSet.sol	a64e5d0e83019d9caa51e6fe6f68ac54b583ac15792b8557cb8e4fab20711b9f
@openzeppelin/contracts/utils/math/SignedMath.sol	420a5a5d8d94611a04b39d6cf5f02492552ed4257ea82aba3c765b1ad52f77f6
@openzeppelin/contracts/utils/math/Math.sol	85a2caf3bd06579fb55236398c1321e15fd524a8fe140dff748c0f73d7a52345
@openzeppelin/contracts/utils/introspection/IERC165.sol	701e025d13ec6be09ae892eb029cd83b3064325801d73654847a5fb11c58b1e5
@openzeppelin/contracts/utils/introspection/ERC165.sol	8806a632d7b656cadb8133ff8f2acae4405b3a64d8709d93b0fa6a216a8a6154
@openzeppelin/contracts/token/ERC20/IERC20.sol	7ebde70853ccafcf1876900dad458f46eb9444d591d39bfc58e952e2582f5587
@openzeppelin/contracts/token/ERC20/ERC20.sol	d20d52b4be98738b8aa52b5bb0f88943f62128969b33d654fbca731539a7fe0a
@openzeppelin/contracts/token/ERC20/extensions/IERC20Metadata.sol	af5c8a77965cc82c33b7ff844deb9826166689e55dc037a7f2f790d057811990
@openzeppelin/contracts/token/ERC20/extensions/ERC20Pausable.sol	9c68903fdd3d113f683b70f78c25c3757e8efbe753663f099db934db09eae74d
@openzeppelin/contracts/security/Pausable.sol	2072248d2f79e661c149fd6a6593a8a3f038466557c9b75e50e0b001bcb5cf97
@openzeppelin/contracts/access/IAccessControlEnumerable.sol	655ab8dc2a9617376734d04ca293e099cc24f8ce893997e68c29cfebc4a61d39
@openzeppelin/contracts/access/IAccessControl.sol	d03c1257f2094da6c86efa7aa09c1c07ebd33dd31046480c5097bc2542140e45
@openzeppelin/contracts/access/AccessControlEnumerable.sol	47861db7fa8d98b58cef570e7c8fca6af6d9d82e3ec0f525c3ad035cbfbed195

@openzeppelin/contracts/access/AccessControl.sol	afd98330d27bddff0db7cb8fcf42bd4766dda5f60b40871a3bec6220f9c9edf7

Overview

The contract is an implementation of an ERC20 token for the R-DEE protocol, named Radiologex token (RDGX). It is built using OpenZeppelin contracts and includes standard ERC20 functionalities and additional features such as pre-minting the total supply to the owner's address at contract creation and incorporating roles for pausing and denying token transfers. Specifically, it introduces a pauser role that can stop all token transfers and a denier role that can prevent token transfers for specific addresses. The contract ensures the owner is granted the default admin role, enabling them to assign these pauser and denier roles to others. This setup is designed to support the R-DEE token sale, emphasizing security and administrative flexibility within the token's ecosystem.

Roles

Denier

The `DENIER_ROLE` role address has authority over the following functions:

- function allow
- function deny

Admin

The `DEFAULT_ADMIN_ROLE` role address has authority over the following functions:

- function grantRole
- function revokeRole

Pauser

The `PAUSER_ROLE` role address has authority over the following functions:

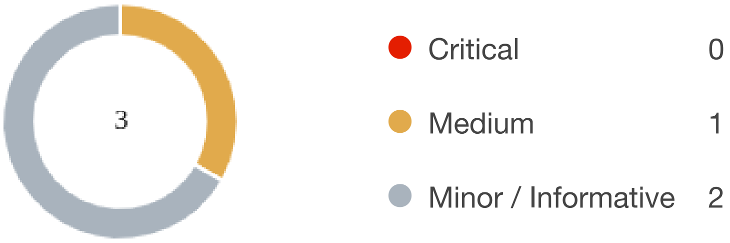
- function pause
- function unpause

Users

The users have the ability to interact with the following functions:

- function transfer
- function transferFrom

Findings Breakdown



Severity		Unresolved	Acknowledged	Resolved	Other
●	Critical	0	0	0	0
●	Medium	1	0	0	0
●	Minor / Informative	2	0	0	0

Diagnostics

● Critical ● Medium ● Minor / Informative

everity	Code	Description	Status
●	BC	Blacklists Addresses	Unresolved
●	ST	Stops Transactions	Unresolved
●	L04	Conformance to Solidity Naming Conventions	Unresolved

BC - Blacklists Addresses

Criticality	Medium
Location	contracts/RDGXToken.sol#L158,208
Status	Unresolved

Description

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

```
   function deny(address _addr) external onlyRole(DENIER_ROLE) {
        if (denylist[_addr])
            revert AlreadyDenied(_addr);

        denylist[_addr] = true;

        emit Denied(_addr);
    }

    function _beforeTokenTransfer(address _from, address _to,
uint256 _amount) internal virtual override {
        if (denylist[_from])
            revert DeniedAddress(_from);
        if (denylist[_to])
            revert DeniedAddress(_to);

        super._beforeTokenTransfer(_from, _to, _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.

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.

ST - Stops Transactions

Criticality	Minor / Informative
Location	contracts/RDGXToken.sol#L129
Status	Unresolved

Description

The contract owner has the authority to stop the transfers for all users including the owner. The owner may pause the transactions by calling the `pause` method.

```
    function pause() external onlyRole(PAUSER_ROLE) {
        _pause();
    }
```

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.

L04 - Conformance to Solidity Naming Conventions

Criticality	Minor / Informative
Location	contracts/RDGXToken.sol#L158,179
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 _addr
```

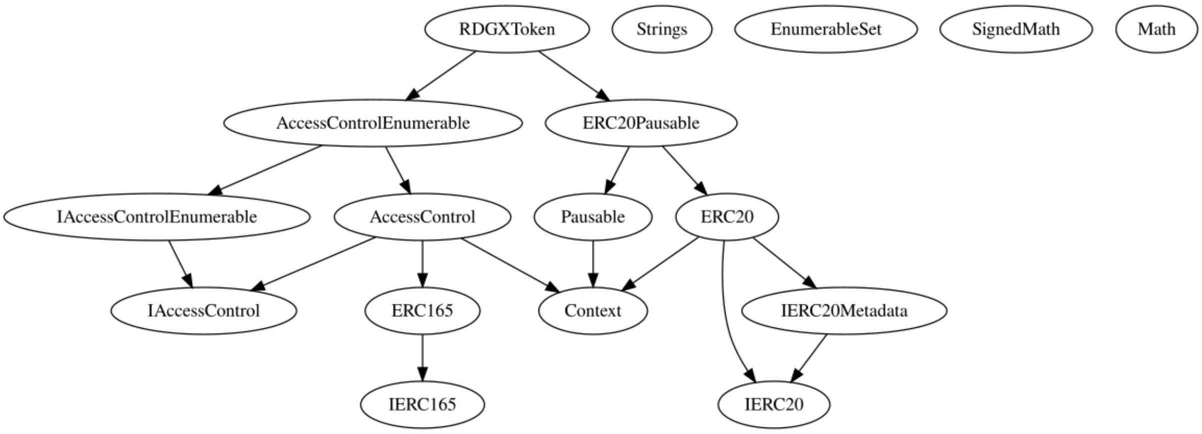
Recommendation

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.

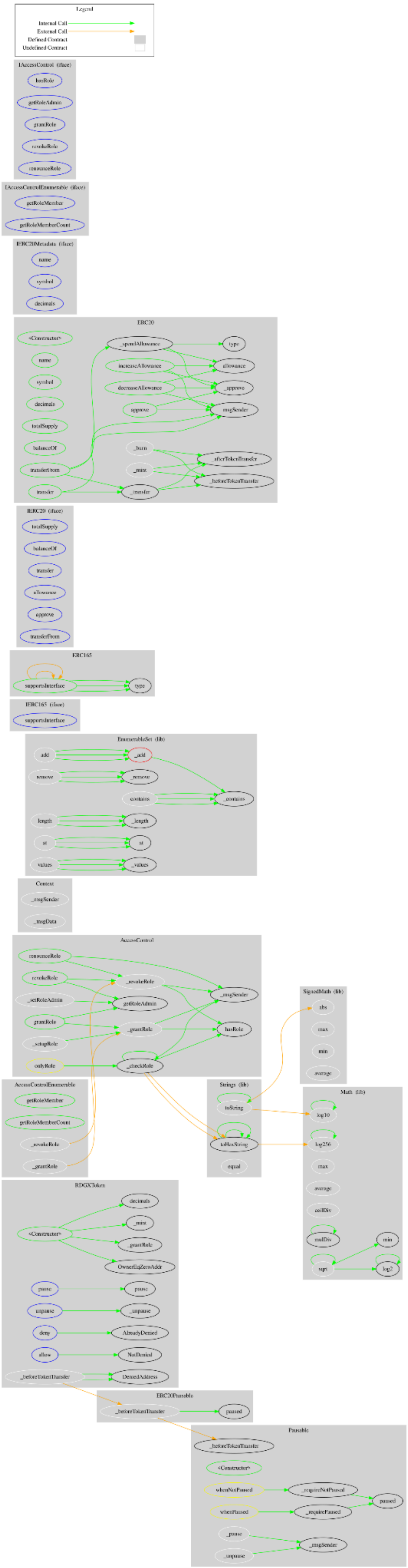
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
RDGXToken	Implementation	AccessControlEnumerable, ERC20Pausable		
		Public	✓	ERC20
	pause	External	✓	onlyRole
	unpause	External	✓	onlyRole
	deny	External	✓	onlyRole
	allow	External	✓	onlyRole
	_beforeTokenTransfer	Internal	✓	

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
IAccessControl (iface)
hasRole
getRoleAdmin
grantRole
revokeRole
renounceRole
IAccessControlEnumerable (iface)
getRoleMember
getRoleMemberCount
IERC20Metadata (iface)
name
symbol
decimals
ERC20
<Constructor>
name
symbol
decimals
totalSupply
balanceOf
transferFrom
transfer
_spendAllowance
increaseAllowance
decreaseAllowance
approve
_burn
_mint
_transfer
type
allowance
_approve
msgSender
_afterTokenTransfer
_beforeTokenTransfer
IERC20 (iface)
totalSupply
balanceOf
transfer
allowance
approve
transferFrom
ERC165
supportsInterface
type
IERC165 (iface)
supportsInterface
EnumerableSet (lib)
add
remove
contains
length
at
values
_add
_remove
_contains
_length
_at
_values
Context
_msgSender
_msgData
AccessControl
renounceRole
revokeRole
_setRoleAdmin
grantRole
_setupRole
onlyRole
_revokeRole
getRoleAdmin
_grantRole
_checkRole
_msgSender
hasRole
SignedMath (lib)
abs
max
min
average
AccessControlEnumerable
getRoleMember
getRoleMemberCount
_revokeRole
_grantRole
Strings (lib)
toString
toHexString
equal
Math (lib)
log10
log256
max
average
ceilDiv
mulDiv
sqrt
min
log2
RDGXToken
<Constructor>
decimals
_mint
_grantRole
OwnerEqZeroAddr
pause
_pause
unpause
_unpause
deny
AlreadyDenied
allow
NotDenied
_beforeTokenTransfer
DeniedAddress
ERC20Pausable
_beforeTokenTransfer
paused
Pausable
_beforeTokenTransfer
<Constructor>
whenNotPaused
_requireNotPaused
whenPaused
_requirePaused
_pause
_unpause
paused
_msgSender

Summary

R-DEE Protocol contract implements a token mechanism. This audit investigates security issues, business logic concerns, and potential improvements.

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