Cyberscope

Audit Report

ParadiseChain

June 2024

Network	ETH
Address	0xf4194164e26e114ef13ccb9a363f338f83c207a6
Audited by	© cyberscope

Table of Contents

Review

Contract Name	Token
Compiler Version	v0.8.20+commit.a1b79de6
Optimization	200 runs
Explorer	https://etherscan.io/address/0xf4194164e26e114ef13ccb9a363f338f83c207a6
Address	0xf4194164e26e114ef13ccb9a363f338f83c207a6
Network	ETH
Symbol	$PARCHA
Decimals	18

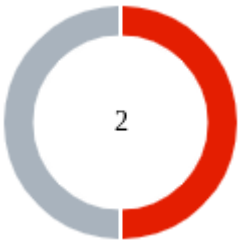
Audit Updates

Initial Audit	24 Apr 2024 https://github.com/cyberscope-io/audits/blob/main/hj/v1/audit.pdf
Corrected Phase 2	14 May 2024 https://github.com/cyberscope-io/audits/blob/main/hj/v2/audit.pdf
Corrected Phase 3	15 May 2024 https://github.com/cyberscope-io/audits/blob/main/hj/v3/audit.pdf
Corrected Phase 4	05 Jun 2024

Source Files

Filename	SHA256
contracts/ParadiseToken.sol	a040d3989a5c429283f67ac00440388934 7d58fdea05b379e91c8a9c716f2e18

Findings Breakdown



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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
●	MT	Mints Tokens	Acknowledged
●	L14	Uninitialized Variables in Local Scope	Unresolved

MT - Mints Tokens

Criticality	Critical
Location	contracts/Token.sol#L44
Status	Acknowledged

Description

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

```
    function setTgePassed() external onlyOwner {
        if (tgeTimestamp != 0) {
            revert TGEisAlreadyPassed();
        }
        tgeTimestamp = block.timestamp;
        uint256 length = allocations.length;
        for (uint256 i; i < length;) {
            _mint(allocations[i].recipient,
allocations[i].amount);
            unchecked {
                ++i;
            }
        }
        emit TGEPassed();
        emit TGETimestampUpdated(tgeTimestamp);
    }
```

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.
- Invoke the `setTgePassed` function.

Team Update

The team states: *We can't start* `setTgePassed` *function right now, because vesting has not started and will be set at a later date.*

L14 - Uninitialized Variables in Local Scope

Criticality	Minor / Informative
Location	contracts/Token.sol#L36,50
Status	Unresolved

Description

Using an uninitialized local variable can lead to unpredictable behavior and potentially cause errors in the contract. It's important to always initialize local variables with appropriate values before using them.

```
uint256 i
```

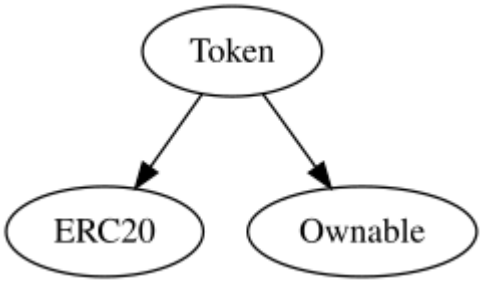
Recommendation

By initializing local variables before using them, the contract ensures that the functions behave as expected and avoid potential issues.

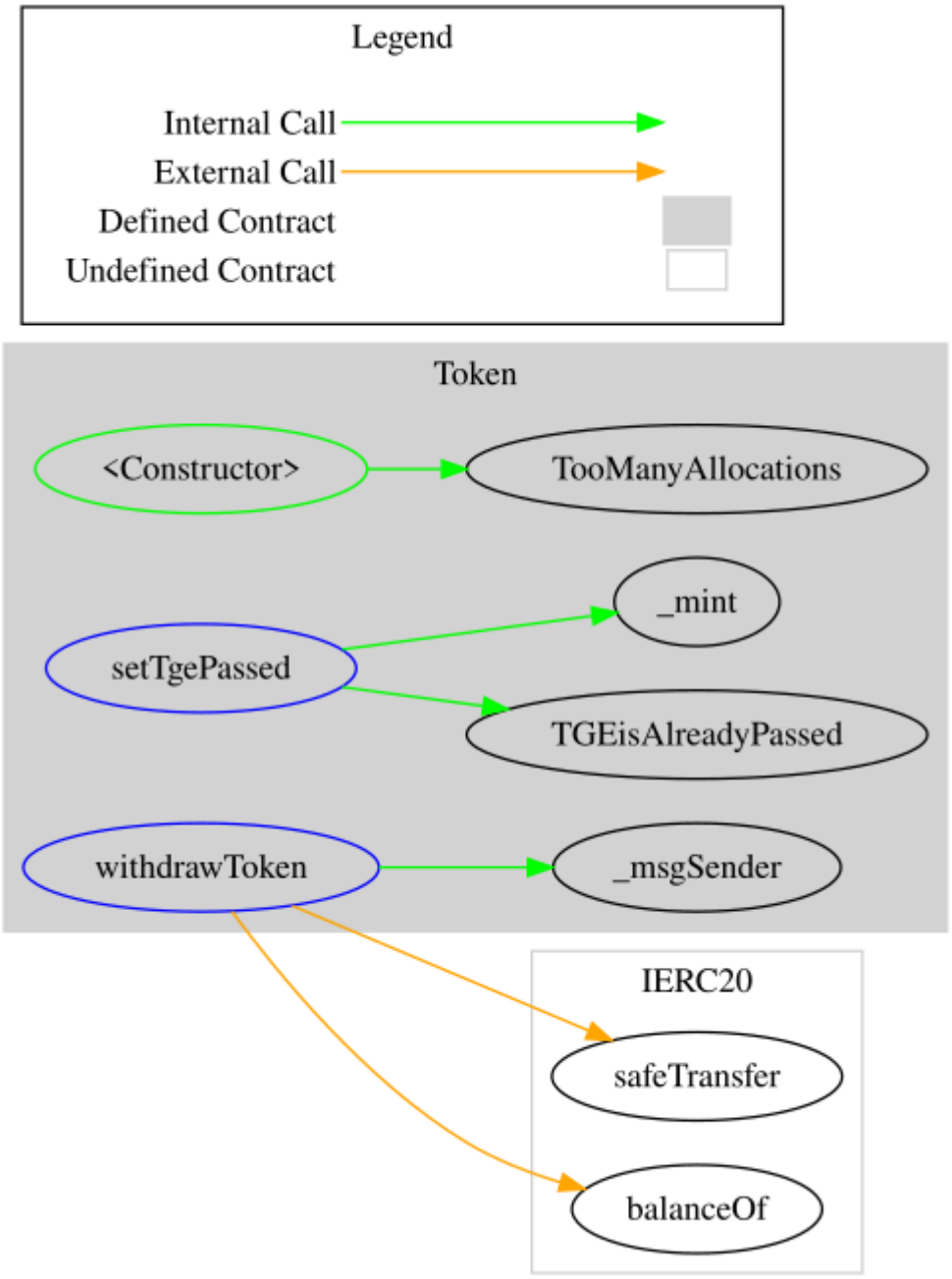
Functions Analysis

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Token	Implementation	ERC20, Ownable		
		Public	✓	ERC20 Ownable
	setTgePassed	External	✓	onlyOwner
	withdrawToken	External	✓	onlyOwner

Inheritance Graph



Flow Graph


Legend
Internal Call
External Call
Defined Contract
Undefined Contract
Token
<Constructor>
TooManyAllocations
_mint
setTgePassed
TGEisAlreadyPassed
withdrawToken
_msgSender
IERC20
safeTransfer
balanceOf

Summary

ParadiseChain 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. The team has acknowledged the finding. 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