Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	Legend Token
Website:	belegends.com
Platform:	Ethereum and Polygon
Language:	Solidity
Date:	August 28th, 2023

Table of contents

Email: audit@EtherAuthority.io

`

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

EtherAuthority was contracted by the Legend team to perform the Security audit of the Legend Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on August 28th, 2023.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

- The LegendToken contract is an ERC20 implementation of the LEGEND utility token on the LEVERADE platform.
- The token is burnable, and the owner can pause transfers/burns as part of an emergency response.
- The smart contracts have functions like pause, unpause, burn, etc.

Audit scope

Name	**Code Review and Security Analysis Report for Legend Token Smart Contract**
Platform	**Ethereum and Polygon / Solidity**
File	LegendToken.sol
Github commit hash	98a41c0e39ba185665d8a3ea0e40450b4374134c
Audit Date	August 28th, 2023

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: Legend • Symbol: LEGEND • Decimals: 18 • Total Supply: 1 billion	**YES, This is valid.**
Ownership Control: • The owner can pause the token transfer. • The owner can resume the token transfer. • Owner can renounce ownership. • Current owner can transfer the ownership.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **“Secured”**. This token contract does contain owner control, which does not make it fully decentralized.

We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 0 low and 1 very low level issues.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Passed
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 1 smart contract. Smart contract contains Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in Legend Token are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Legend Token.

The Legend Token team has provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Code parts are **well** commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a Legend Token smart contract code in the form of a github web link. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **well** commented.And The logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official project URL: https://www.belegends.com/#token-section which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	pause	write	The owner can pause the token transfer	Refer Audit Findings
3	unpause	write	access only Owner	No Issue
4	_beforeTokenTransfer	internal	Passed	No Issue
5	name	read	Passed	No Issue
6	symbol	read	Passed	No Issue
7	decimals	read	Passed	No Issue
8	totalSupply	read	Passed	No Issue
9	balanceOf	read	Passed	No Issue
10	transfer	write	Passed	No Issue
11	allowance	read	Passed	No Issue
12	approve	write	Passed	No Issue
13	transferFrom	write	Passed	No Issue
14	increaseAllowance	write	Passed	No Issue
15	decreaseAllowance	write	Passed	No Issue
16	_transfer	internal	Passed	No Issue
17	_update	internal	Passed	No Issue
18	_mint	internal	Passed	No Issue
19	_burn	internal	Passed	No Issue
20	_approve	internal	Passed	No Issue
21	_approve	internal	Passed	No Issue
22	_spendAllowance	internal	Passed	No Issue
23	burn	write	Passed	No Issue
24	burnFrom	write	Passed	No Issue
25	whenNotPaused	modifier	Passed	No Issue
26	whenPaused	modifier	Passed	No Issue
27	paused	write	Passed	No Issue
28	_requireNotPaused	internal	Passed	No Issue
29	_requirePaused	internal	Passed	No Issue
30	_pause	internal	Passed	No Issue
31	_unpause	internal	Passed	No Issue
32	onlyOwner	modifier	Passed	No Issue
33	owner	read	Passed	No Issue
34	_checkOwner	internal	Passed	No Issue
35	renounceOwnership	write	access only Owner	No Issue
36	transferOwnership	write	access only Owner	No Issue
37	_transferOwnership	internal	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) The owner can pause the token transfer:
The owner can pause the token transfer anytime. This may lead to centralization risk. If the private key gets stolen or the owner intentionally stops the transfer/burn of the tokens, then users' tokens will get stuck as he cannot use his tokens.

Resolution: We suggest confirming this feature.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

LegendToken.sol

- pause: Owner can pause token transfers.
- unpause: Owner can resume token transfers.

Ownable.sol

- renounceOwnership: Deleting ownership will leave the contract without an owner, removing any owner-only functionality.
- transferOwnership: Current owner can transfer ownership of the contract to a new account.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of a github web link. And we have used all possible tests based on given objects as files. We had observed 1 informational issue in the smart contracts. But that is not a critical one. So, **it's good to go for the production**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed smart contract, based on standard audit procedure scope, is **"Secured".**

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

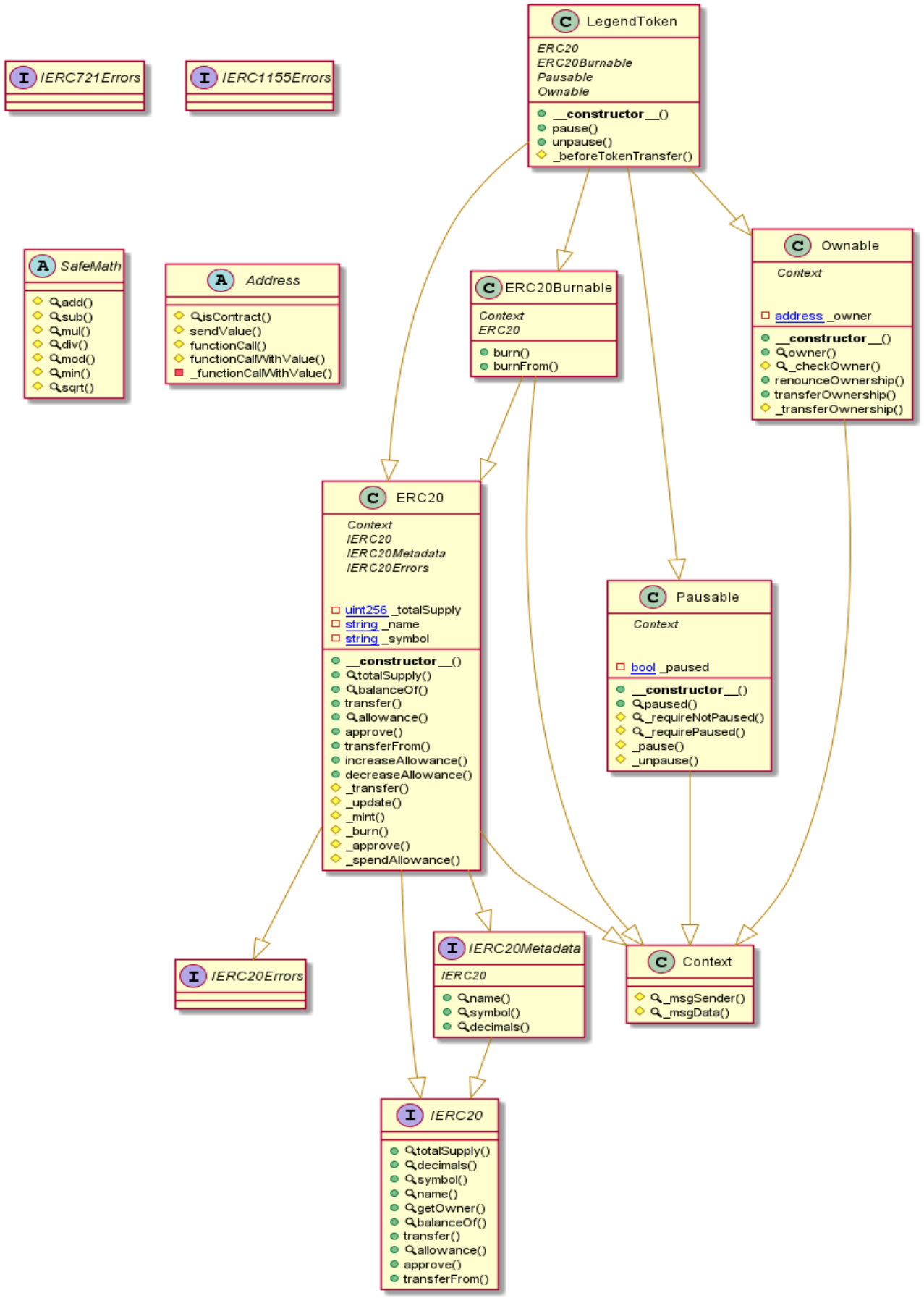
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Legend Token



Slither Results Log

Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

Slither Log >> LegendToken.sol

```
Address.isContract(address) (LegendToken.sol#94-101) uses assembly
        - INLINE ASM (LegendToken.sol#97-99)
Address._functionCallWithValue(address,bytes,uint256,string) (LegendToken.sol#140-162) uses assembly
        - INLINE ASM (LegendToken.sol#154-157)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage

Address._functionCallWithValue(address,bytes,uint256,string) (LegendToken.sol#140-162) is never used and should be removed
Address.functionCall(address,bytes) (LegendToken.sol#110-112) is never used and should be removed
Address.functionCall(address,bytes,string) (LegendToken.sol#114-120) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256) (LegendToken.sol#122-128) is never used and should be removed
Address.functionCallWithValue(address,bytes,uint256,string) (LegendToken.sol#130-138) is never used and should be removed
Address.isContract(address) (LegendToken.sol#94-101) is never used and should be removed
Address.sendValue(address,uint256) (LegendToken.sol#103-108) is never used and should be removed
Context._msgData() (LegendToken.sol#199-202) is never used and should be removed
ERC20._mint(address,uint256) (LegendToken.sol#309-314) is never used and should be removed
LegendToken._beforeTokenTransfer(address,address,uint256) (LegendToken.sol#469-475) is never used and should be removed
SafeMath.add(uint256,uint256) (LegendToken.sol#15-20) is never used and should be removed
SafeMath.div(uint256,uint256) (LegendToken.sol#48-50) is never used and should be removed
SafeMath.div(uint256,uint256,string) (LegendToken.sol#52-61) is never used and should be removed
SafeMath.min(uint256,uint256) (LegendToken.sol#76-78) is never used and should be removed
SafeMath.mod(uint256,uint256) (LegendToken.sol#63-65) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (LegendToken.sol#67-74) is never used and should be removed
SafeMath.mul(uint256,uint256) (LegendToken.sol#37-46) is never used and should be removed
SafeMath.sqrt(uint256) (LegendToken.sol#80-91) is never used and should be removed
SafeMath.sub(uint256,uint256) (LegendToken.sol#22-24) is never used and should be removed
SafeMath.sub(uint256,uint256,string) (LegendToken.sol#26-35) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
```

```
Pragma version^0.8.9 (LegendToken.sol#2) allows old versions
solc-0.8.9 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in Address.sendValue(address,uint256) (LegendToken.sol#103-108):
        - (success) = recipient.call{value: amount}() (LegendToken.sol#106)
Low level call in Address._functionCallWithValue(address,bytes,uint256,string) (LegendToken.sol#140-162):
        - (success,returndata) = target.call{value: weiValue}(data) (LegendToken.sol#148)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls

Redundant expression "this (LegendToken.sol#200)" inContext (LegendToken.sol#194-203)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements

LegendToken (LegendToken.sol#456-477) does not implement functions:
        - IERC20Metadata.decimals() (LegendToken.sol#210)
        - IERC20.getOwner() (LegendToken.sol#173)
        - IERC20Metadata.name() (LegendToken.sol#206)
        - IERC20Metadata.symbol() (LegendToken.sol#208)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
LegendToken.sol analyzed (13 contracts with 84 detectors), 28 result(s) found
```

Solidity Static Analysis

LegendToken.sol

Gas costs:

Gas requirement of function LegendToken.pause is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 26:4:

Gas costs:

Gas requirement of function LegendToken.unpause is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 33:4:

Constant/View/Pure functions:

LegendToken._beforeTokenTransfer(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 40:4:

Solhint Linter

LegendToken.sol

```
Compiler version ^0.8.9 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:1
global import of path @openzeppelin/contracts/token/ERC20/ERC20.sol
is not allowed. Specify names to import individually or bind all
exports of the module into a name (import "path" as Name)
Pos: 1:3
global import of path
@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol is
not allowed. Specify names to import individually or bind all exports
of the module into a name (import "path" as Name)
Pos: 1:4
global import of path @openzeppelin/contracts/security/Pausable.sol
is not allowed. Specify names to import individually or bind all
exports of the module into a name (import "path" as Name)
Pos: 1:5
global import of path @openzeppelin/contracts/access/Ownable.sol is
not allowed. Specify names to import individually or bind all exports
of the module into a name (import "path" as Name)
Pos: 1:6
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:18
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Email: audit@EtherAuthority.io