Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Crolend Token
Platform: Cronos Chain
Language: Solidity
Date: October 1st, 2022

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 Crolend Token team to perform the Security audit of the Crolend 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 October 1st, 2022.

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

Crolend Token is an ERC20 token having functionalities like token vesting, delegate, delegates, etc.

Audit scope

Name	**Code Review and Security Analysis Report for Crolend Token Smart Contract**
Platform	**Cronos Chain / Solidity**
File	Token.sol
File MD5 Hash	3C14F60C55E7472280B34BD966518329
Updated File MD5 Hash	84872EA72EE1587EE711028ACA913603
Updated Online Code Link	0x34deb73e57f7be74d2cca1869d2c721e16c7a32c
Audit Date	October 1st, 2022
Revised Audit Date	October 8th, 2022

Email: audit@EtherAuthority.io

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: ● Name: Crolend ● Symbol: CRD ● Decimals: 18 ● Maximum Supply: 1 billion ● Total Supply: 1 billion	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity based smart contracts are **“Secured”**. This token contract does not contain owner control, which does 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 some very low level issues.

All the issues have been fixed / acknowledged in the revised code.

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**

Email: audit@EtherAuthority.io

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 the Crolend 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 Crolend Token.

The Crolend Token team has **not** 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 used, which is a good thing.

Documentation

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

As mentioned above, code parts are well commented on. 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.

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 not used in external smart contract calls.

AS-IS overview

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Missing require error messages	Refer Audit Findings
2	__mint	internal	Passed	No Issue
3	delegates	external	Passed	No Issue
4	_transfer	internal	Passed	No Issue
5	delegate	external	Passed	No Issue
6	delegateBySig	external	Passed	No Issue
7	getCurrentVotes	external	Passed	No Issue
8	getPriorVotes	external	Passed	No Issue
9	_delegate	internal	Passed	No Issue
10	_moveDelegates	internal	Passed	No Issue
11	_writeCheckpoint	internal	Passed	No Issue
12	safe32	internal	Passed	No Issue
13	getChainId	internal	Passed	No Issue
14	owner	read	Passed	No Issue
15	onlyOwner	modifier	Passed	No Issue
16	renounceOwnership	write	access only Owner	No Issue
17	transferOwnership	write	access only Owner	No Issue
18	name	read	Passed	No Issue
19	symbol	read	Passed	No Issue
20	decimals	read	Passed	No Issue
21	totalSupply	read	Passed	No Issue
22	balanceOf	read	Passed	No Issue
23	transfer	write	Passed	No Issue
24	allowance	read	Passed	No Issue
25	approve	write	Passed	No Issue
26	transferFrom	write	Passed	No Issue
27	increaseAllowance	write	Passed	No Issue
28	decreaseAllowance	write	Passed	No Issue
29	_transfer	internal	Passed	No Issue
30	_mint	internal	Passed	No Issue
31	_burn	internal	Passed	No Issue
32	_approve	internal	Passed	No Issue
33	_setupDecimals	internal	Passed	No Issue
34	_beforeTokenTransfer	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

(1) Division before multiplication:

```
__mint(msg.sender, MAX_SUPPLY / 100 * 20);
__mint(address(communityLockToken), MAX_SUPPLY / 100 * 10);
__mint(address(adLockToken), MAX_SUPPLY / 100 * 10);
__mint(address(idoLockToken), MAX_SUPPLY / 100 * 5);
__mint(address(teamLockToken), MAX_SUPPLY / 100 * 5);
__mint(lend_, MAX_SUPPLY / 100 * 50);
```

Solidity being resource constrained language, dividing any amount and then multiplying will cause discrepancies in the outcome. Therefore always multiply the amount first and then divide it.

Resolution: Consider ordering multiplication before division.
Status: Fixed

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Multiple pragma:

There are multiple pragmas with different compiler versions.

Resolution: We suggest using only one pragma and removing the other.

Status: Acknowledged

(2) No need to use SafeMath library for solidity version over 0.8.0:

```
using SafeMath for uint256;
```

The solidity version over 0.8.0 has an in-built overflow / underflow prevention mechanism. And thus, the explicit use of SathMath library is not necessary. It saves some gas as well.

Status: Acknowledged

(3) Missing require error messages:

```
constructor(
    address _beneficiary,
    uint256 _start,
    uint256 _cliff,
    uint256 _duration
) {
    require(_beneficiary != address(0));
    require(_cliff <= _duration);
```

There are some places in contract where require has been used for validation, but error message has not been mentioned.

Resolution: We suggest adding an error message.It is helpful to get failure of the transaction.

Status: Acknowledged

Conclusion

We were given a contract code in the form of a cronoscan.com link and we have used all possible tests based on given objects as files. We have observed some Informational issues in the token smart contract. All the issues have been fixed / acknowledged in the revised code. So, **it's good to go for the mainnet deployment**.

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.

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

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

Email: audit@EtherAuthority.io

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).

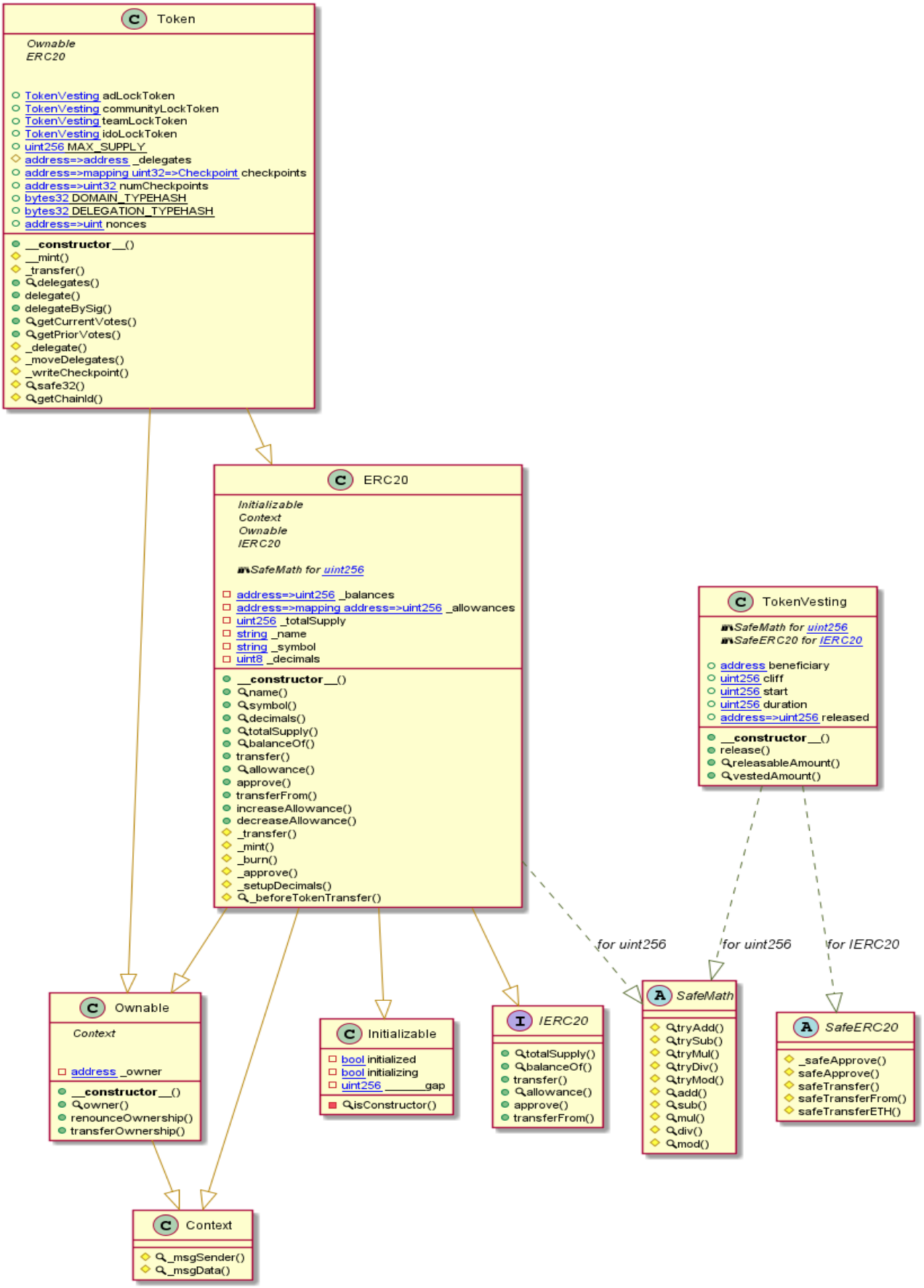
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we 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 - Crolend Token



Slither Results Log

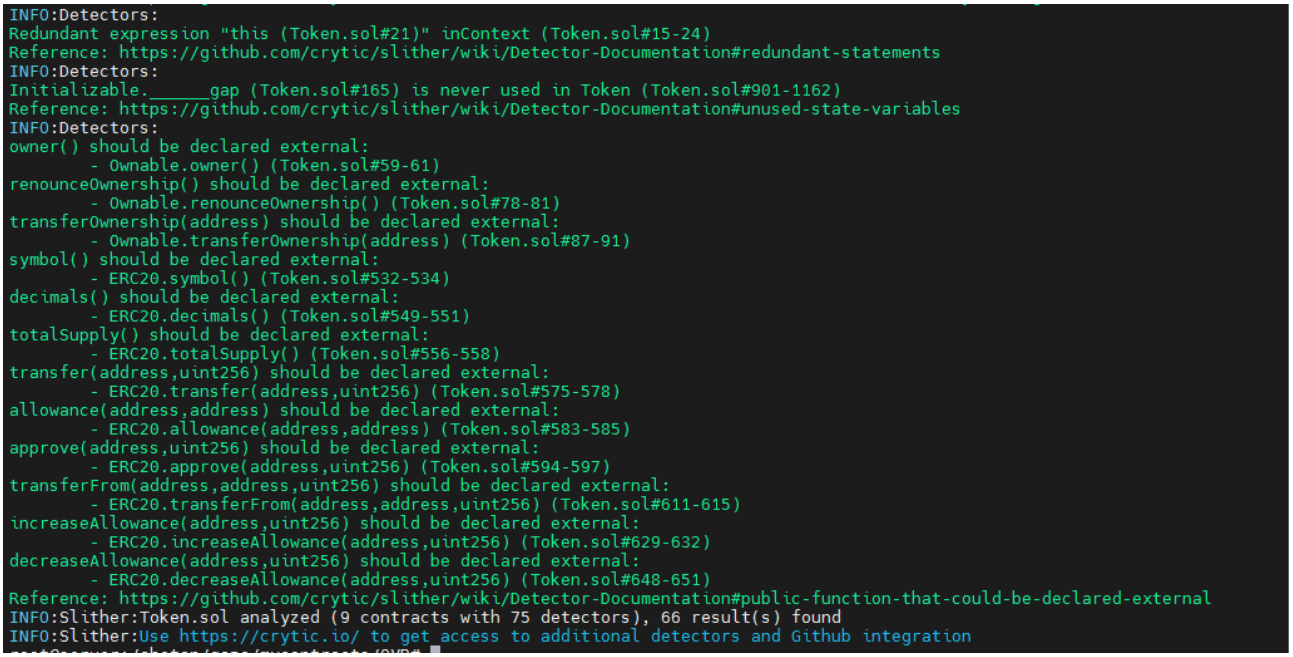
Slither Log >> Token.sol

```
INFO:Detectors:
ERC20.allowance(address,address).owner (Token.sol#583) shadows:
        - Ownable.owner() (Token.sol#59-61) (function)
ERC20._approve(address,address,uint256).owner (Token.sol#731) shadows:
        - Ownable.owner() (Token.sol#59-61) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Reentrancy in TokenVesting.release(address) (Token.sol#855-865):
        External calls:
        - IERC20(token).safeTransfer(beneficiary,unreleased) (Token.sol#862)
        Event emitted after the call(s):
        - Released(unreleased) (Token.sol#864)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
TokenVesting.release(address) (Token.sol#855-865) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool)(unreleased > 0) (Token.sol#858)
TokenVesting.vestedAmount(address) (Token.sol#881-893) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp < cliff (Token.sol#886)
        - block.timestamp >= start.add(duration) (Token.sol#888)
Token.delegateBySig(address,uint256,uint8,bytes32,bytes32) (Token.sol#997-1038) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp <= expiry,FarmToken::delegateBySig: signature expired) (Token.sol#1036)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Initializable.isConstructor() (Token.sol#152-162) uses assembly
        - INLINE ASM (Token.sol#160)
Token.getChainId() (Token.sol#1156-1160) uses assembly
        - INLINE ASM (Token.sol#1158)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Different versions of Solidity is used:
        - Version used: ['>=0.6.0', '>=0.6.0<0.9.0', '^0.8.0']
        - >=0.6.0<0.9.0 (Token.sol#3)
        - >=0.6.0<0.9.0 (Token.sol#28)
        - >=0.6.0<0.9.0 (Token.sol#95)
        - >=0.6.0<0.9.0 (Token.sol#169)
        - ^0.8.0 (Token.sol#247)
        - >=0.6.0<0.9.0 (Token.sol#462)
        - >=0.6.0 (Token.sol#769)
        - ^0.8.0 (Token.sol#802)
        - ^0.8.0 (Token.sol#897)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used
```

```
INFO:Detectors:
Context._msgData() (Token.sol#20-23) is never used and should be removed
ERC20._burn(address,uint256) (Token.sol#708-716) is never used and should be removed
ERC20._setupDecimals(uint8) (Token.sol#746-748) is never used and should be removed
Initializable.isConstructor() (Token.sol#152-162) is never used and should be removed
SafeERC20._safeApprove(IERC20,address,uint256) (Token.sol#773-777) is never used and should be removed
SafeERC20.safeApprove(IERC20,address,uint256) (Token.sol#778-781) is never used and should be removed
SafeERC20.safeTransferETH(address,uint256) (Token.sol#795-798) is never used and should be removed
SafeERC20.safeTransferFrom(IERC20,address,address,uint256) (Token.sol#789-793) is never used and should be removed
SafeMath.div(uint256,uint256,string) (Token.sol#430-435) is never used and should be removed
SafeMath.mod(uint256,uint256) (Token.sol#394-396) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (Token.sol#452-457) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (Token.sol#265-271) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (Token.sol#307-312) is never used and should be removed
SafeMath.tryMod(uint256,uint256) (Token.sol#319-324) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (Token.sol#290-300) is never used and should be removed
SafeMath.trySub(uint256,uint256) (Token.sol#278-283) is never used and should be removed
Token._transfer(address,address,uint256) (Token.sol#927-930) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version>=0.6.0<0.9.0 (Token.sol#3) is too complex
Pragma version>=0.6.0<0.9.0 (Token.sol#28) is too complex
Pragma version>=0.6.0<0.9.0 (Token.sol#95) is too complex
Pragma version>=0.6.0<0.9.0 (Token.sol#169) is too complex
Pragma version^0.8.0 (Token.sol#247) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version>=0.6.0<0.9.0 (Token.sol#462) is too complex
Pragma version>=0.6.0 (Token.sol#769) allows old versions
Pragma version^0.8.0 (Token.sol#802) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
Pragma version^0.8.0 (Token.sol#897) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
Low level call in SafeERC20._safeApprove(IERC20,address,uint256) (Token.sol#773-777):
        - (success,data) = address(token).call(abi.encodeWithSelector(0x095ea7b3,to,value)) (Token.sol#775)
Low level call in SafeERC20.safeTransfer(IERC20,address,uint256) (Token.sol#783-787):
        - (success,data) = address(token).call(abi.encodeWithSelector(0xa9059cbb,to,value)) (Token.sol#785)
Low level call in SafeERC20.safeTransferFrom(IERC20,address,address,uint256) (Token.sol#789-793):
        - (success,data) = address(token).call(abi.encodeWithSelector(0x23b872dd,from,to,value)) (Token.sol#791)
Low level call in SafeERC20.safeTransferETH(address,uint256) (Token.sol#795-798):
        - (success) = to.call{value: value}(new bytes(0)) (Token.sol#796)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Variable Initializable._____gap (Token.sol#165) is not in mixedCase
Function Token.__mint(address,uint256) (Token.sol#923-926) is not in mixedCase
Parameter Token.__mint(address,uint256)._to (Token.sol#923) is not in mixedCase
Parameter Token.__mint(address,uint256)._amount (Token.sol#923) is not in mixedCase
Variable Token._delegates (Token.sol#939) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
```



Solidity Static Analysis

Token.sol

Security

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

more

Pos: 160:4:

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

more

Pos: 1158:8:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

more

Pos: 1036:16:

Low level calls:

Use of "call": should be avoided whenever possible. It can lead to unexpected behavior if return value is not handled properly. Please use Direct Calls via specifying the called contract's interface.

more

Pos: 796:26:

Gas & Economy

Gas costs:

Gas requirement of function Token.getCurrentVotes 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: 1045:4:

Gas costs:

Gas requirement of function Token.getPriorVotes 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: 1061:4:

Miscellaneous

Email: audit@EtherAuthority.io

Constant/View/Pure functions:

Token.getChainId() : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1156:4:

Similar variable names:

Token._writeCheckpoint(address,uint32,uint256,uint256) : Variables have very similar names "numCheckpoints" and "nCheckpoints". Note: Modifiers are currently not considered by this static analysis.
Pos: 1145:12:

Similar variable names:

Token._writeCheckpoint(address,uint32,uint256,uint256) : Variables have very similar names "numCheckpoints" and "nCheckpoints". Note: Modifiers are currently not considered by this static analysis.
Pos: 1145:40:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1066:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1152:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 920:22:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 1086:36:

Solhint Linter

Token.sol

```
Token.sol:266:18: Error: Parse error: missing ';' at '{'
Token.sol:279:18: Error: Parse error: missing ';' at '{'
Token.sol:291:18: Error: Parse error: missing ';' at '{'
Token.sol:308:18: Error: Parse error: missing ';' at '{'
Token.sol:320:18: Error: Parse error: missing ';' at '{'
Token.sol:412:18: Error: Parse error: missing ';' at '{'
Token.sol:431:18: Error: Parse error: missing ';' at '{'
Token.sol:453:18: Error: Parse error: missing ';' at '{'
```

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