



X528 Contract, Code Review and Security Analysis Report

Customer: X528
Prepared on: 22nd December 2022
Platform: Binance
Language: Solidity

rdauditors.com

Table of Contents

Disclaimer	2
Document	3
Introduction	4
Project Scope	5
Executive Summary	6
Code Quality	6
Documentation	8
Use of Dependencies	8
AS-IS Overview	9
Code Flow Diagram - C528Token.sol	10
Code Flow Diagram - Slither Results Log	11
Audit Findings	18
Conclusion	19
Note For Contract Users	20
Our Methodology	21
Disclaimers	23

Disclaimer

This document may contain confidential information about its systems and intellectual property of the customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the customer or it can be disclosed publicly after all vulnerabilities are fixed - upon the decision of the customer.

Document

Name	Smart Contract Code Review and Security Analysis Report of X528
Platform	Binance/ Solidity
File	C528Token..sol
MD5 hash	1785058a7161f784b8811e9252d311a1
SHA256 hash	41e38567e49b4e91dac1cbb0bbe2184f4fd288b427d30e645bee181cc8e15ff4
Date	22/12/2022

Introduction

RD Auditors (Consultant) were contracted by X528 (Customer) to conduct a Smart Contract Code Review and Security Analysis. This report represents the findings of the security assessment of the customer`s smart contract and its code review conducted between 20th - 22nd December 2022.

This contract consists of one file.

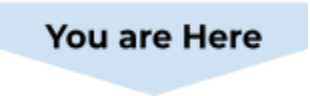
Project Scope

The scope of the project is a smart contract. We have scanned this smart contract for commonly known and more specific vulnerabilities, below are those considered (the full list includes but is not limited to):


- Reentrancy
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Byte array vulnerabilities
- Style guide violation
- Transfer forwards all gas
- ERC20 API violation
- Malicious libraries
- Compiler version not fixed
- Unchecked external call - Unchecked math
- Unsafe type inference
- Implicit visibility level


Executive Summary

According to the assessment, the customer's solidity smart contract is now **Well-Secured**.




You are Here

 Insecure






 Poorly Secured

 Secure

 Well-Secured

Automated checks are with smartDec, Mythril, Slither and remix IDE. All issues were performed by our team, which included the analysis of code functionality, the manual audit found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the audit overview section. The general overview is presented in the AS-IS section and all issues found are located in the audit overview section.

We found the following;

Total Issues	0
 Critical	0
 High	0
 Medium	0
 Low	0
 Very Low	0

Code Quality

The libraries within this smart contract are part of a 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 to a specific address and its properties/methods can be reused many times by other contracts.

The Crypto528 team has not provided scenario and unit test scripts, which would help to determine the integrity of the code in an automated way.

Overall, the code is almost commented. Commenting can provide rich documentation for functions, return variables and more. Use of the Ethereum Natural Language Specification Format (NatSpec) for commenting is recommended.

Documentation

We were given the X528 code as a Github link:

<https://github.com/magduf/C528Token/tree/main/c528Token-v03-truffle-gov/contracts>

The hash of that file is mentioned in the table. As mentioned above, it's recommended to write comments on smart contract code, so anyone can quickly understand the programming flow as well as complex code logic.

Comments are very helpful in understanding the overall architecture of the protocol. It also provides a clear overview of the system components, including helpful details, like the lifetime of the background script.

Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure. Those were based on well known industry standard open source projects and even core code blocks that are written well and systematically.

AS-IS Overview

C528Token.sol

File And Function Level Report

Inherit: ERC20, ERC20Permit, ERC20Votes, AccessControl

Observation: Passed

Test Report: Passed

Sl.	Function	Type	Observation	Test Report	Conclusion	Score
1	burn	public	Passed	All Passed	No Issue	Passed
2	setOnWhitelis t	external	Passed	All Passed	No Issue	Passed
3	setInRequire WhitelistMod e	external	Passed	All Passed	No Issue	Passed
4	withdrawToke n	external	Passed	All Passed	No Issue	Passed
5	_beforeTokenT ransfer	internal	Passed	All Passed	No Issue	Passed
6	_afterTokenTra nsfer	internal	Passed	All Passed	No Issue	Passed
7	_mint	internal	Passed	All Passed	No Issue	Passed
8	_burn	internal	Passed	All Passed	No Issue	Passed

Code Flow Diagram - Slither Results Log

C528Token.sol

```

INFO:Detectors:
ERC20.allowance(address,address).owner (C528Token.sol#1100) shadows:
  - Ownable.owner() (C528Token.sol#1030-1032) (function)
ERC20._approve(address,address,uint256).owner (C528Token.sol#1172) shadows:
  - Ownable.owner() (C528Token.sol#1030-1032) (function)
ERC20Permit.constructor(string).name (C528Token.sol#1202) shadows:
  - ERC20.name() (C528Token.sol#1075-1077) (function)
  - IERC20.name() (C528Token.sol#986) (function)
ERC20Permit.permit(address,address,uint256,uint256,uint8,bytes32,bytes32).owner (C528Token.sol#1205) shadows:
  - Ownable.owner() (C528Token.sol#1030-1032) (function)
ERC20Permit.nonces(address).owner (C528Token.sol#1225) shadows:
  - Ownable.owner() (C528Token.sol#1030-1032) (function)
ERC20Permit._useNonce(address).owner (C528Token.sol#1233) shadows:
  - Ownable.owner() (C528Token.sol#1030-1032) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Variable 'ERC20Votes._moveVotingPower(address,address,uint256).newWeight (C528Token.sol#1377)' in ERC20Votes._moveVotingPower(
address,address,uint256) (C528Token.sol#1370-1386) potentially used before declaration: (oldWeight,newWeight) = _writeCheckpoi
nt(_checkpoints[dst],_add,amount) (C528Token.sol#1382)
Variable 'ERC20Votes._moveVotingPower(address,address,uint256).oldWeight (C528Token.sol#1377)' in ERC20Votes._moveVotingPower(
address,address,uint256) (C528Token.sol#1370-1386) potentially used before declaration: (oldWeight,newWeight) = _writeCheckpoi
nt(_checkpoints[dst],_add,amount) (C528Token.sol#1382)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#pre-declaration-usage-of-local-variables
INFO:Detectors:
ERC20Permit.permit(address,address,uint256,uint256,uint8,bytes32,bytes32) (C528Token.sol#1204-1223) uses timestamp for comparis
ons
  Dangerous comparisons:
  - require(bool,string)(block.timestamp <= deadline,ERC20Permit: expired deadline) (C528Token.sol#1213)
ERC20Votes.delegateBySig(address,uint256,uint256,uint8,bytes32,bytes32) (C528Token.sol#1315-1332) uses timestamp for compariso
ns
  Dangerous comparisons:
  - require(bool,string)(block.timestamp <= expiry,ERC20Votes: signature expired) (C528Token.sol#1323)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp

```

```

INFO:Detectors:
Strings.toString(uint256) (C528Token.sol#8-26) uses assembly
  - INLINE ASM (C528Token.sol#13-15)
  - INLINE ASM (C528Token.sol#18-20)
ECDSA.tryRecover(bytes32,bytes) (C528Token.sol#72-86) uses assembly
  - INLINE ASM (C528Token.sol#77-81)
Math.mulDiv(uint256,uint256,uint256) (C528Token.sol#553-606) uses assembly
  - INLINE ASM (C528Token.sol#561-565)
  - INLINE ASM (C528Token.sol#575-580)
  - INLINE ASM (C528Token.sol#584-590)
Address.isContract(address) (C528Token.sol#909-916) uses assembly
  - INLINE ASM (C528Token.sol#912-914)
Address.functionCallWithValue(address,bytes,uint256,string) (C528Token.sol#955-977) uses assembly
  - INLINE ASM (C528Token.sol#969-972)
ERC20Votes._unsafeAccess(ERC20Votes.Checkpoint[],uint256) (C528Token.sol#1419-1424) uses assembly
  - INLINE ASM (C528Token.sol#1420-1423)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage

```

```
INFO:Detectors:
Pragma version^0.8.4 (C528Token.sol#2) 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 Address.sendValue(address,uint256) (C528Token.sol#918-923):
- (success) = recipient.call{value: amount}() (C528Token.sol#921)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (C528Token.sol#955-977):
- (success,returndata) = target.call{value: weiValue}(data) (C528Token.sol#963)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Variable EIP712._CACHED_DOMAIN_SEPARATOR (C528Token.sol#769) is not in mixedCase
Variable EIP712._CACHED_CHAIN_ID (C528Token.sol#770) is not in mixedCase
Variable EIP712._CACHED_THIS (C528Token.sol#771) is not in mixedCase
Variable EIP712._HASHED_NAME (C528Token.sol#773) is not in mixedCase
Variable EIP712._HASHED_VERSION (C528Token.sol#774) is not in mixedCase
Variable EIP712._TYPE_HASH (C528Token.sol#775) is not in mixedCase
Function IERC20Permit.DOMAIN_SEPARATOR() (C528Token.sol#826) is not in mixedCase
Function ERC20Permit.DOMAIN_SEPARATOR() (C528Token.sol#1229-1231) is not in mixedCase
Variable ERC20Permit._PERMIT_TYPEHASH_DEPRECATED_SLOT (C528Token.sol#1200) is not in mixedCase
Parameter C528Token.setOnWhitelist(address,bool)._address (C528Token.sol#1629) is not in mixedCase
Parameter C528Token.setOnWhitelist(address,bool)._isActive (C528Token.sol#1629) is not in mixedCase
Parameter C528Token.setInRequireWhitelistMode(bool)._inRequireWhitelistMode (C528Token.sol#1635) is not in mixedCase
Parameter C528Token.withdrawToken(address,address,uint256)._token (C528Token.sol#1643) is not in mixedCase
Parameter C528Token.withdrawToken(address,address,uint256)._account (C528Token.sol#1643) is not in mixedCase
Parameter C528Token.withdrawToken(address,address,uint256)._amount (C528Token.sol#1643) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
```

```
INFO:Detectors:
Redundant expression "this (C528Token.sol#1014)" inContext (C528Token.sol#1009-1017)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements
INFO:Detectors:
C528Token.constructor() (C528Token.sol#1616-1620) uses literals with too many digits:
- _mint(msg.sender,250000000 * 10 ** 18) (C528Token.sol#1617)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
ERC20Permit._PERMIT_TYPEHASH_DEPRECATED_SLOT (C528Token.sol#1200) is never used in C528Token (C528Token.sol#1608-1675)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variables
INFO:Detectors:
ERC20Permit._PERMIT_TYPEHASH_DEPRECATED_SLOT (C528Token.sol#1200) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Slither:C528Token.sol analyzed (22 contracts with 75 detectors), 155 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

C528Token.sol

Gas & Economy

Gas costs:

Gas requirement of function C528Token.burn 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: 28:4:

Gas costs:

Gas requirement of function C528Token.withdrawToken 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: 59:4:

Similar variable names:

C528Token.withdrawToken(address,address,uint256) : Variables have very similar names "_account" and "_amount". Note: Modifiers are currently not considered by this static analysis.

Pos: 62:36:

Similar variable names:

C528Token.withdrawToken(address,address,uint256) : Variables have very similar names "_account" and "_amount". Note: Modifiers are currently not considered by this static analysis.

Pos: 62:46:

Similar variable names:

C528Token._burn(address,uint256) : Variables have very similar names "account" and "amount". Note: Modifiers are currently not considered by this static analysis.

Pos: 96:20:

Similar variable names:

C528Token._burn(address,uint256) : Variables have very similar names "account" and "amount". Note: Modifiers are currently not considered by this static analysis.

Pos: 96:29:

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: 30:8:

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: 44:8:

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: 50:8:

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: 60:8:

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: 71:12:

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to lost tokens etc.
High	High level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g. public access to crucial functions.
Medium	Medium level vulnerabilities are important to fix; however, they cannot lead to lost tokens.
Low	Low level vulnerabilities are most related to outdated, unused etc. These code snippets cannot have a significant impact on execution.
Lowest Code Style/ Best Practice	Lowest level vulnerabilities, code style violations and information statements cannot affect smart contract execution and can be ignored.

Audit Findings

Critical:

No critical severity vulnerabilities were found.

High:

No high severity vulnerabilities were found.

Medium:

No medium severity vulnerabilities were found.

Low:

No low severity vulnerabilities were found.

Very Low:

No very low severity vulnerabilities were found.

Conclusion

We were given a contract file and have used all possible tests based on the given object. So it is now ready for mainnet deployment. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

The security state of the reviewed contract is “**Well-Secured**”.

Note For Contract Users

There are several owner only functions. Those can be called by the owner's wallet only. So, if the owner's wallet is compromised, then it carries the risk of the contract becoming vulnerable.

Owner has full control over the smart contract. Thus, technical auditing does not guarantee the project's ethical side.

Please do your due diligence before investing. Our audit report is never an investment advice.

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 analyse 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 scrutinised 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

RD Auditors Disclaimer

The smart contracts given for audit have been analysed 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).

Because the total number of test cases are unlimited, the audit makes no statements or warranties on the 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 recommend proceeding with several independent audits and a public bug bounty program to ensure security of smart contracts.

Technical Disclaimer

Smart contracts are deployed and executed on the blockchain. 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.



Email: info@rdauditors.com

Website: www.rdauditors.com

