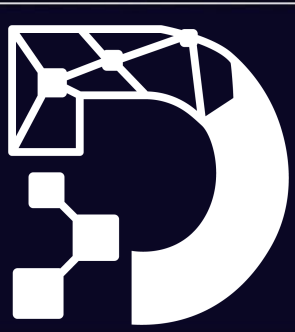
ASSURE DEFI®
THE VERIFICATION GOLD STANDARD

Security Assessment:

Destra Network Token

March 28, 2024

- Audit Status: **Pass**
- Audit Edition: **Advance**



Risk Analysis

Classifications of Manual Risk Results

Classification	Description
Critical	Danger or Potential Problems.
High	Be Careful or Fail test.
Low	Pass, Not-Detected or Safe Item.
Informational	Function Detected

Manual Code Review Risk Results

Contract Privilege	Description
Buy Tax	5%
Sale Tax	5%
Cannot Buy	Pass
Cannot Sale	Pass
Max Tax	100%
Modify Tax	Yes
Fee Check	Pass
Is Honeypot?	Not Detected
Trading Cooldown	Not Detected
Can Pause Trade?	Fail
Pause Transfer?	Detected
Max Tx?	Pass
Is Anti Whale?	Not Detected
Is Anti Bot?	Not Detected

Contract Privilege	Description
Is Blacklist?	Detected
Blacklist Check	Fail
is Whitelist?	Detected
Can Mint?	Pass
Is Proxy?	Not Detected
Can Take Ownership?	Not Detected
Hidden Owner?	Not Detected
Owner	0x9CE77c36570A2BDA5B94b8Df092Dd26abbDF4589
Self Destruct?	Not Detected
External Call?	Not Detected
Other?	Not Detected
Holders	1
Auditor Confidence	Low Risk
KYC Present	No
KYC URL	

The following quick summary it's added to the project overview; however, there are more details about the audit and its results. Please read every detail.

Project Overview

Token Summary

Parameter	Result
Address	0xf94e7d0710709388bCe3161C32B4eEA56d3f91CC
Name	Destra Network
Token Tracker	Destra Network (DSync)
Decimals	18
Supply	1,000,000,000
Platform	ETHEREUM
compiler	v0.8.17+commit.8df45f5f
Contract Name	DestraNetwork
Optimization	Yes with 200 runs
LicenseType	MIT
Language	Solidity
Codebase	https://etherscan.io/address/0xf94e7d0710709388bCe3161C32B4eEA56d3f91CC#code
Payment Tx	Corporate

Main Contract Assessed
Contract Name

Name	Contract	Live
Destra Network	0xf94e7d0710709388bCe3161C32B4eEA56d3f91CC	Yes

TestNet Contract was Not Assessed

Solidity Code Provided

SolID	File Sha-1	FileName
DSync	8bf85430c367e99b1a5abd321198f93d90442cf8	DSync.sol
DSync		
DSync		
DSync		
DSync		
DSync	undefined	

Smart Contract Vulnerability Checks

The Smart Contract Weakness Classification Registry (SWC Registry) is an implementation of the weakness classification scheme proposed in EIP-1470. It is loosely aligned to the terminologies and structure used in the Common Weakness Enumeration (CWE) while overlaying a wide range of weakness variants that are specific to smart contracts.

ID	Severity	Name	File	location
SWC-100	Pass	Function Default Visibility	DSync.sol	L: 0 C: 0
SWC-101	Pass	Integer Overflow and Underflow.	DSync.sol	L: 0 C: 0
SWC-102	Pass	Outdated Compiler Version file.	DSync.sol	L: 0 C: 0
SWC-103	Pass	A floating pragma is set.	DSync.sol	L: 0 C: 0
SWC-104	Pass	Unchecked Call Return Value.	DSync.sol	L: 0 C: 0
SWC-105	Pass	Unprotected Ether Withdrawal.	DSync.sol	L: 0 C: 0
SWC-106	Pass	Unprotected SELFDESTRUCT Instruction	DSync.sol	L: 0 C: 0
SWC-107	Pass	Read of persistent state following external call.	DSync.sol	L: 0 C: 0
SWC-108	Pass	State variable visibility is not set..	DSync.sol	L: 0 C: 0
SWC-109	Pass	Uninitialized Storage Pointer.	DSync.sol	L: 0 C: 0
SWC-110	Pass	Assert Violation.	DSync.sol	L: 0 C: 0
SWC-111	Pass	Use of Deprecated Solidity Functions.	DSync.sol	L: 0 C: 0
SWC-112	Pass	Delegate Call to Untrusted Callee.	DSync.sol	L: 0 C: 0
SWC-113	Pass	Multiple calls are executed in the same transaction.	DSync.sol	L: 0 C: 0
SWC-114	Pass	Transaction Order Dependence.	DSync.sol	L: 0 C: 0

ID	Severity	Name	File	location
SWC-115	Pass	Authorization through tx.origin.	DSync.sol	L: 0 C: 0
SWC-116	Pass	A control flow decision is made based on The block.timestamp environment variable.	DSync.sol	L: 0 C: 0
SWC-117	Pass	Signature Malleability.	DSync.sol	L: 0 C: 0
SWC-118	Pass	Incorrect Constructor Name.	DSync.sol	L: 0 C: 0
SWC-119	Pass	Shadowing State Variables.	DSync.sol	L: 0 C: 0
SWC-120	Pass	Potential use of block.number as source of randonmness.	DSync.sol	L: 0 C: 0
SWC-121	Pass	Missing Protection against Signature Replay Attacks.	DSync.sol	L: 0 C: 0
SWC-122	Pass	Lack of Proper Signature Verification.	DSync.sol	L: 0 C: 0
SWC-123	Pass	Requirement Violation.	DSync.sol	L: 0 C: 0
SWC-124	Pass	Write to Arbitrary Storage Location.	DSync.sol	L: 0 C: 0
SWC-125	Pass	Incorrect Inheritance Order.	DSync.sol	L: 0 C: 0
SWC-126	Pass	Insufficient Gas Griefing.	DSync.sol	L: 0 C: 0
SWC-127	Pass	Arbitrary Jump with Function Type Variable.	DSync.sol	L: 0 C: 0
SWC-128	Pass	DoS With Block Gas Limit.	DSync.sol	L: 0 C: 0
SWC-129	Pass	Typographical Error.	DSync.sol	L: 0 C: 0
SWC-130	Pass	Right-To-Left-Override control character (U +202E).	DSync.sol	L: 0 C: 0
SWC-131	Pass	Presence of unused variables.	DSync.sol	L: 0 C: 0
SWC-132	Pass	Unexpected Ether balance.	DSync.sol	L: 0 C: 0

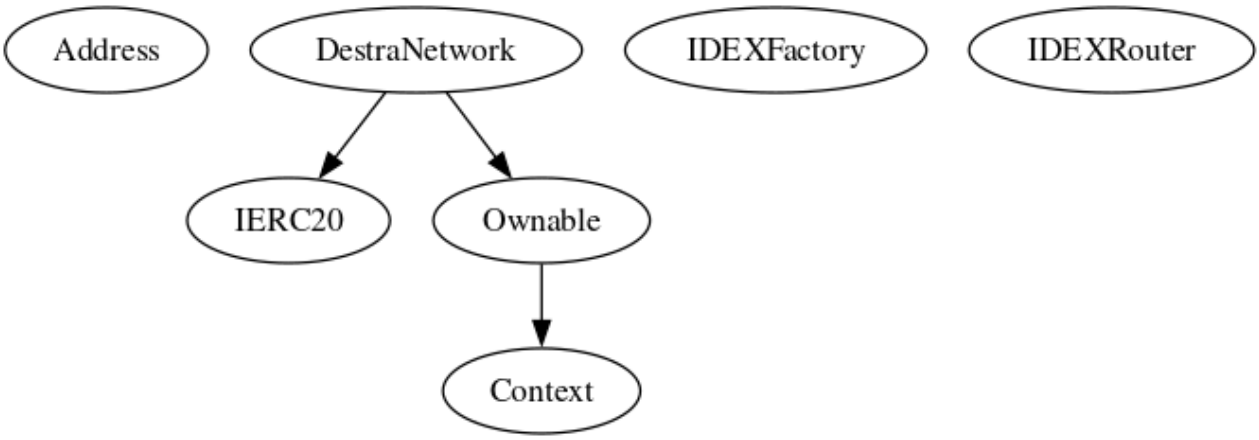
ID	Severity	Name	File	location
SWC-133	Pass	Hash Collisions with Multiple Variable Length Arguments.	DSync.sol	L: 0 C: 0
SWC-134	Pass	Message call with hardcoded gas amount.	DSync.sol	L: 0 C: 0
SWC-135	Pass	Code With No Effects (Irrelevant/Dead Code).	DSync.sol	L: 0 C: 0
SWC-136	Pass	Unencrypted Private Data On-Chain.	DSync.sol	L: 0 C: 0

We scan the contract for additional security issues using MYTHX and industry-standard security scanning tools.

Inheritance

The contract for Destra Network has the following inheritance structure.

The Project has a Total Supply of 1,000,000,000



Privileged Functions (onlyOwner)

Please Note if the contract is Renounced none of this functions can be executed.

Function Name	Parameters	Visibility
renounceOwnership		Public
transferOwnership	address newOwner	Public
setTeamMember		External
airdrop		External
clearStuckBalance		External
blacklistWallets		External
openTrading		External
addLiquidityPool		External
setSwapBackRateLimit		External
setTxLimit		External
setMaxWallet		External
setIsFeeExempt		External
setIsTxLimitExempt		External
setFees		External
toggleTransferTax		External
setFeeReceivers		External

Function Name	Parameters	Visibility
setSwapBackSettings		External

DSync-01 | Potential Sandwich Attacks.

Category	Severity	Location	Status
Security	Medium	DSync.sol: L: 488, C: 14	Detected

Description

A sandwich attack might happen when an attacker observes a transaction swapping tokens or adding liquidity without setting restrictions on slippage or minimum output amount. The attacker can manipulate the exchange rate by frontrunning (before the transaction being attacked) a transaction to purchase one of the assets and make profits by back running (after the transaction being attacked) a transaction to sell the asset. The following functions are called without setting restrictions on slippage or minimum output amount, so transactions triggering these functions are vulnerable to sandwich attacks, especially when the input amount is large:

- swapExactTokensForETHSupportingFeeOnTransferTokens()
- addLiquidityETH()

Remediation

We recommend setting reasonable minimum output amounts, instead of 0, based on token prices when calling the aforementioned functions.

Referrences:

What Are Sandwich Attacks in DeFi — and How Can You Avoid Them?.

DSync-16 | Taxes can be up to 100%.

Category	Severity	Location	Status
Logical Issue	Critical	DSync.sol: L: 714 C: 14	Detected

Description

The current definition of taxes can be set up to 100% for specific wallets, we suggest to modify the function not to be dynamic but to be a static resolution.

feeInTokens > senderBalance &&
(feeInTokens / 100) * 95 <= senderBalance

due to the logic written in here may results in loss of funds.

Remediation

We advise the team to review the following logic function function setFee(uint256 redisFeeOnBuy, uint256 redisFeeOnSell, uint256 taxFeeOnBuy, uint256 taxFeeOnSell) public onlyOwner {
    _redisFeeOnBuy = redisFeeOnBuy;
    _redisFeeOnSell = redisFeeOnSell;
    _taxFeeOnBuy = taxFeeOnBuy;
    _taxFeeOnSell = taxFeeOnSell;
}

Project Action

Technical Findings Summary

Classification of Risk

Severity	Description
Critical	Risks are those that impact the safe functioning of a platform and must be addressed before launch. Users should not invest in any project with outstanding critical risks.
High	Risks can include centralization issues and logical errors. Under specific circumstances, these major risks can lead to loss of funds and/or control of the project.
Medium	Risks may not pose a direct risk to users' funds, but they can affect the overall functioning of a platform
Low	Risks can be any of the above but on a smaller scale. They generally do not compromise the overall integrity of the Project, but they may be less efficient than other solutions.
Informational	Errors are often recommended to improve the code's style or certain operations to fall within industry best practices. They usually do not affect the overall functioning of the code.

Findings

Severity	Found	Pending	Resolved
Critical	1	1	0
High	0	0	0
Medium	1	1	0
Low	0	0	0
Informational	0	0	0
Total	2	2	0

Social Media Checks

Social Media	URL	Result
Twitter	https://x.com/destranetwork	Pass
Other		N/A
Website	https://destra.network	Pass
Telegram	https://t.me/DestraNetwork	Pass

We recommend to have 3 or more social media sources including a completed working websites.

Social Media Information Notes:

Auditor Notes: undefined

Project Owner Notes:

Audit Result

Final Audit Score

Review	Score
Security Score	85
Auditor Score	85

The Following Score System Has been Added to this page to help understand the value of the audit, the maximum score is 100, however to attain that value the project most pass and provide all the data needed for the assessment. Our Passing Score has been changed to 85 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below.

Audit Passed

Assessment Results

Important Notes:

- Audit override.

Auditor Score =85
Audit Passed

Appendix

Finding Categories

Centralization / Privilege

Centralization / Privilege findings refer to either feature logic or implementation of components that actagainst the nature of decentralization, such as explicit ownership or specialized access roles incombination with a mechanism to relocate funds.

Gas Optimization

Gas Optimization findings do not affect the functionality of the code but generate different, more optimalEVM opcodes resulting in a reduction on the total gas cost of a transaction.

Logical Issue

Logical Issue findings detail a fault in the logic of the linked code, such as an incorrect notion on howblock.timestamp works.

Control Flow

Control Flow findings concern the access control imposed on functions, such as owner-only functionsbeing invoke-able by anyone under certain circumstances.

Volatile Code

Volatile Code findings refer to segments of code that behave unexpectedly on certain edge cases that mayresult in a vulnerability.

Coding Style

Coding Style findings usually do not affect the generated byte-code but rather comment on how to makethe codebase more legible and, as a result, easily maintainable.

Inconsistency

Inconsistency findings refer to functions that should seemingly behave similarly yet contain different code,such as a constructor assignment imposing different require statements on the input variables than a setterfunction.

Coding Best Practices

ERC 20 Conding Standards are a set of rules that each developer should follow to ensure the code meet a set of creterias and is readable by all the developers.

Disclaimer

Assure Defi has conducted an independent security assessment to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the reviewed code for the scope of this assessment. This report does not constitute agreement, acceptance, or advocation for the Project, and users relying on this report should not consider this as having any merit for financial advice in any shape, form, or nature. The contracts audited do not account for any economic developments that the Project in question may pursue, and the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude, and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are entirely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence, regardless of the findings presented. Information is provided ‘as is, and Assure Defi is under no covenant to audited completeness, accuracy, or solidity of the contracts. In no event will Assure Defi or its partners, employees, agents, or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions or actions with regards to the information provided in this audit report.

The assessment services provided by Assure Defi are subject to dependencies and are under continuing development. You agree that your access 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 with high levels of technical risk and uncertainty. The assessment reports could include false positives, negatives, and unpredictable results. The services may access, and depend upon, multiple layers of third parties.