Assure DeFi®

THE VERIFICATION **GOLD STANDARD**

Security Assessment

OPAL

Date: 04/10/2025

Audit Status: PASS

Audit Edition: Advanced

ASSURE DEFI®

THE VERIFICATION GOLD STANDARD

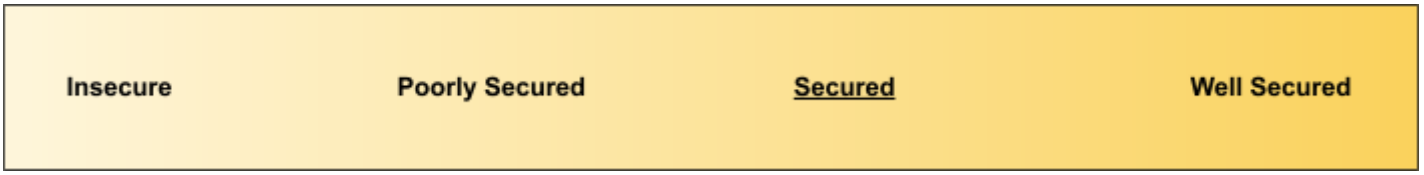
Risk Analysis

Vulnerability summary

Classification	Description
High	High-level vulnerabilities can result in the loss of assets or manipulation of data.
Medium	Medium-level vulnerabilities can be challenging to exploit, but they still have a considerable impact on smart contract execution, such as allowing public access to critical functions.
Low	Low-level vulnerabilities are primarily associated with outdated or unused code snippets that generally do not significantly impact execution, sometimes they can be ignored.
Informational	Informational vulnerabilities, code style violations, and informational statements do not affect smart contract execution and can typically be disregarded.

Executive Summary

According to the Assure assessment, the Customer's smart contract is **Secured.**



Scope

Target Code And Revision

For this audit, we performed research, investigation, and review of the OPAL contracts followed by issue reporting, along with mitigation and remediation instructions outlined in this report.

Target Code And Revision

Project	Assure
Language	Solidity
Codebase	https://etherscan.io/token/0x199E2CFaf8B4f2CC5423971EF3749d1c89Cf815C#code
Audit Methodology	Static, Manual

Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

Category	Item
Code review & Functional Review	• Compiler warnings. • Race conditions and Reentrancy. • Cross-function race conditions. • Possible delays in data delivery. • Oracle calls. • Front running. • Timestamp dependence. • Integer Overflow and Underflow. • DoS with Revert. • DoS with block gas limit. • Methods execution permissions. • Economy model. • Private user data leaks. • Malicious Event log. • Scoping and Declarations. • Uninitialized storage pointers. • Arithmetic accuracy. • Design Logic. • Cross-function race conditions. • Safe Zeppelin module. • Fallback function security. • Overpowered functions / Owner privileges

AUDIT OVERVIEW

HIGH

No high severity issues were found.

MEDIUM

1. Conditional sell freeze via unpayable taxWallet

Function: _swapTokens (ETH forward), _update (swap trigger), updateTaxWallet

Issue: When auto-swap triggers, the contract swaps fee tokens for ETH and then forwards all ETH to taxWallet via a low-level call with require(success). If the owner sets taxWallet to a non-payable/reverting contract, that call always fails and any transfer that triggers a swap (typically sells) reverts, effectively freezing sells while the fee buffer ≥ threshold.

Recommendation: Do not revert on failed ETH forward. Use a pull model (tax wallet withdraws), or make forwarding best-effort (log on failure, retain ETH). Optionally enforce that taxWallet is a payable EOA or add validation in updateTaxWallet or renounce Ownership.

2. Irreversible “market pair” flag enables targeted taxation/griefing

Function: setMarketPair, marketPairs mapping

Issue: The owner can set any address as a market pair once; there’s no way to unset due to PairAlreadySet() on repeat. Marking an EOA makes transfers to it taxed as sells and from it taxed as buys permanently, enabling targeted fee/grief behavior.

Recommendation: Allow both set and unset of pair status, or restrict to verified DEX pairs (factory/codehash checks). Consider time-lock/2-step change for governance.

3. Owner can force a large dump with amountOutMin=0 (severe price impact risk)

Function: manualSwap, _swapTokens, setTokensForSwap

Issue: manualSwap lets the owner swap the contract's token balance using swapExactTokensForETHSupportingFeeOnTransferTokens with amountOutMin = 0. Combined with a generous cap (maxSwapAmount = tokensForSwap * 20 and tokensForSwap configurable up to 0.5% supply), a single call can dump a very large amount with no slippage protection, causing heavy price impact/MEV exposure.

Recommendation: Lower the cap and/or throttle swaps; tighten the maximum tokensForSwap, introduce non-zero amountOutMin (oracle- or input-based), split large swaps into multiple smaller swaps.

LOW

---

1. External calls in swap path guarded but still a reentrancy surface

Function: _swapTokens (router calls and taxWallet.call{value:..}), lockSwapProcess / inSwapProcess

Issue: Swap path performs external calls; a custom guard (inSwapProcess) prevents classic reentrancy during fee application. Residual risk remains due to arbitrary taxWallet code execution, though current guard and Solidity 0.8 checks meaningfully limit exploitation.

Recommendation: Keep the guard, prefer a pull-payment pattern for taxWallet to remove external calls from the hot path, keep admin functions non-reentrant.

2. Misleading API: getSellTaxPercent() returns basis points

Function: getSellTaxPercent

Issue: The function name implies a percent (for ex 10), but it returns BPS (for example 1000). This can mislead integrators and UIs.

Recommendation: Rename to getSellTaxBps() or return a true percentage (divide by 100 with documented precision).

INFORMATIONAL

No informational issues were found.

Technical Findings Summary

Findings

Vulnerability Level		Total	Pending	Not Apply	Acknowledged	Partially Fixed	Fixed
	HIGH	0					
	MEDIUM	3	3				
	LOW	2	2				
	INFORMATIONAL	0					

Assessment Results

Score Results

Review	Score
Global Score	**85/100**
Assure KYC	Not completed
Audit Score	85/100

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 must pass and provide all the data needed for the assessment. Our Passing Score has been changed to 84 Points for a higher standard, if a project does not attain 85% is an automatic failure. Read our notes and final assessment below. The Global Score is a combination of the evaluations obtained between having or not having KYC and the type of contract audited together with its manual audit.

Audit PASS

Following our comprehensive security audit of the token contract for the OPAL project, the project did meet the necessary criteria required to pass the security audit.

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 advocating for the Project, and users relying on this report should not consider this as having any merit for financial adOPAL 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 adOPAL, nor should it be used to signal that any person 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 audit 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 serOPALs 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 serOPALs, 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 serOPALs may access, and depend upon, multiple layers of third parties.